Joint Service Publication 329
Information Coherence for Defence

Issue 4.0 Version 1.2 - Final
4 July 2011

MINISTRY OF DEFENCE

JSP329 Contents

MINISTRY OF DEFENCE

JSP 329 Version History

Version	Date	Version Information
1.0	1 April 2011	Policy documentation rewritten changing Issue number to 4 version 1. Revision and renaming of Chapter 2 to accommodate the amalgamation of chapters 2, 3 and 5 – MOD Data Definition, Corporate Reference Information (CRI), Annex A (Controlled Values Repository) and UK Defence Terminology Policy to reflect change of terminology and approach to usage of the Controlled Values Repository. Amendment of Contents page plus renumbering and realignment of following chapters reflecting changes including updates of Glossary and Abbreviations. Removal of Enterprise Architecture Policy which has been superseded by JSP 605. Removal of the ERN abbreviations list of values (LoV) from chapter 7 Annex A. LoV now accessible from the CVR via URL link from chapter 7.
1.1	11 May 2011	Inclusion of Unit Identity Number (UIN) – Policy and Management document at chapter 7. Chapters 7 and 8 renumbered following inclusion of the new chapter.
1.2	04 July 2011	Updates made to contact details for Information Coherence Subject Matter Experts (SME) which reflects changes in ICAD's internal staffing structure, brought about by establishment of the Defence Business Services (DBS) organisation. Changes made (to Ch3; Electronic Data Exchange Policy) to emphasise the fact that policy relates to information exchange standards being used by Communication and Information Systems. It is known that some of the standards in the 'Recognised Standards Hierarchy' have been superseded and changes have been made to Ch3, Annex A; Standards Hierarchy which advise readers to seek SME advice before using any standard in the spreadsheet.

MINISTRY OF DEFENCE

JSP 329 Equality And Diversity Statement

Joint Service Publication (JSP) 329 – Information Coherence Policy for Defence, has been assessed using the Equality and Diversity Impact Assessment Tool (EDIAT). It has been identified as having no impact against Gender, Race/Ethnicity, Disability, Sexual Orientation, Religion or Belief, Age and Fair Employment Community Background.

This assessment has been carried out in conjunction with CIO's policy. This policy has been produced in order to:

- **Meet its legal obligations as a Department.**
- **Support the requirements of the Equality and Diversity Scheme.**

MINISTRY OF DEFENCE

JSP 329 Chapter 1
Overview of Information Coherence

Introduction

1. This Policy Set defines how the MOD will manage, exchange and view information by providing a framework for Information Coherence throughout Defence. Within this, users such as Project Teams (PTs) developing Communication Information Systems (CIS), have the freedom to innovate in order to minimise the project whole life costs.

2. JSP 329 has been separated into discrete Policies which may each stand on their own. It is therefore recommended that the publication is entered via the contents page where links are provided to each of the Policies. Depending on individual circumstances it should then be possible to select the particular Policies that apply. However, where any doubt exists, please contact the CIO Information Coherence Policy team for advice.

Background

3. Consistent information is required to support the delivery of Defence capability and, to enable its use to best effect. Our information must be treated and managed as a corporate asset. Defence Information Infrastructure (DII) will provide a common infrastructure, which will aid communications. However, it will not address data interchange, standards or methodologies. Yet Network Enabled Capability (NEC) demands that these issues are addressed in both the business and battle space in order to achieve information sharing leading to information superiority. While not providing all the answers this Policy Set provides an important framework on which information sharing can be built.

4. A key principle of good data management is to "capture once use many times". MOD currently has a huge amount of often competing data stored in a myriad of systems, databases and filing cabinets. This data is widely distributed and, unless controlled and consistently labelled, much will be duplicated and the authoritative source data difficult to find. If information is not properly maintained and understood, it also has the potential to misinform through being out of date; potentially leading to serious operational mistakes such as firing upon the wrong target. Improving the storage, quality, retrieval and coherence of our data therefore requires governance and unambiguous understanding of terminology. These Policies are intended to define the requirements for information sharing within the MOD and, by setting appropriate exchange standards, contribute towards reducing the need for interfaces.

Applicability

5. These Policies apply to any person, project or system that will be storing or exchanging information within the MOD CIS or between the MOD and an external application.

6. There should be no exceptions to this Policy. Legacy projects and programmes will however need to balance benefit against cost of any change. Therefore, unless a significant upgrade is planned, it is not intended that legacy systems undergo extensive rework to comply, although some work may be unavoidable to ensure interoperability between systems.

Key Words

7. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" in this publication, are to be interpreted as follows:

   a. MUST. This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

   b. MUST NOT. This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

   c. SHOULD. This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

   d. SHOULD NOT. This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

   e. MAY. This word, or the adjective "OPTIONAL", mean that an item is truly optional. One area may choose to include the item to meet a particular requirement while another may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides).

8. Changes to the Policy, and the associated guidance are approved by CIO. Any interested party can request a change through the CIO Information Coherence Policy team Tel: 01793 555433 or Mil 96381 5433.

MINISTRY OF DEFENCE

JSP 329 Chapter 2
Authoritative Reference Data Policy

Introduction

1. The use of Authoritative Reference Data[1] will help improve interoperability and information exploitation across Defence, enabling Communication and Information Systems (CIS) and organisations to communicate more effectively.

2. Authoritative Reference Data (ARD) comprises approved Terms, Definitions, List of Values and XML Schema made available through the MOD Controlled Values Repository (CVR). The CVR will either contain the ARD or provide a link to an authoritative source where it can be found. The CVR is regularly updated as new ARD is approved for inclusion. Further information regarding the CVR can be found on the Applications and Tools channel of the Defence Intranet under the Information Policy & Services section.

3. Applications for ARD include;

   a. Terms: for labelling content on CIS to aid information search, storage and retrieval. Commonly referred to as subject categories and keywords and recorded as metadata in document properties. For example keywords and subject categories recorded against SharePoint and Defence Intranet content enable the MOD Enterprise Search engine to return both a more comprehensive set of results and results organised in a more structured manner.

   b. Definitions: used in the production of glossaries and the development of CIS. Where a definition is to be used in CIS development then additional information on Data Type, Length and Format will be captured.

   c. List of Values: to provide controlled values for a user to select from rather than create their own. These are most commonly used in CIS development but equally apply to other data capture formats such as that on forms and templates. For example a list of Military Ranks or International Country Codes.

   d. XML Schema: for the transfer of information used in CIS development and the management of data.

4. Each aspect of ARD is explained in more detail later in the chapter. If further assistance is required, the CIO Information Coherence Policy team can provide support and guidance in the applicability of, and adherence to, this policy. Provision of subject matter expertise on the management and development of ARD and the use of the CVR is provided by Defence Business Services (DBS) through DBS KI-ICAD.

5. This policy is a rationalisation of the Corporate Reference Information (CRI), Data Definition and UK Defence Terminology Policy chapters previously held in JSP 329.

Policy

6. The MOD MUST:

   a. use existing ARD made available through the CVR when developing new, or updating existing, CIS containing information of corporate interest[2];

[1] Reference data that meets agreed quality criteria and is made available through the CVR.

b. make all ARD available through the CVR for wider use and exploitation.

c. Use the UK Defence Terminology (UKDT) to provide the terms for Subject Category and Subject Keyword metadata for MOD wide information management systems.

Applicability

7. There SHOULD be no exceptions to this Policy. Legacy projects and programmes will, however, need to balance benefit against cost of any change. Therefore, unless a significant upgrade is planned, it is not intended that legacy systems undergo extensive rework to comply, although some work may be unavoidable to ensure interoperability between systems.

Compliance Criteria

8. Projects MUST provide evidence that the MOD Authoritative Reference Data Policy is referenced in their User Requirement Document (URD), as either constraints or requirements, at Initial Gate.

9. Projects MUST provide evidence within their System Requirements Document (SRD) that the solution complies with the MOD Authoritative Reference Data Policy by Main Gate.

Reason for Implementation

10. Adherence to the Authoritative Reference Data Policy can benefit the MOD by:

- enabling interoperability between CIS;
- reducing implementation costs for new CIS through the reuse of existing ARD;
- improved exploitation of information resources through the use of consistent ARD;
- creating more efficient management of ARD through a centralised approach;
- removing some of the ambiguity over appropriate use and ownership of data;
- introducing the adoption of common standards with effective ownership and management of data by the appropriate organisations;
- reducing the amount of competing reference data across MOD;
- improving management information and decision making.

Additional Information and Guidance

Terms

11. The use of consistent terminology when labelling documents (descriptive metadata) will help collaborative working and enable the retrieval of information while providing understanding of the context in which it should be used.

12. The MOD provides a set of terms that are used in the labelling of documents on corporate applications including the Defence Intranet, SharePoint and Electronic Records Management Systems (ERMS). These terms are collectively known as the UK Defence Terminology (UKDT) and are available to browse on the Defence Intranet or to download from the CVR. Further details on UKDT can be found in the UK Defence Terminology Guidance.

13. MOD wide information management systems MUST use the UKDT to provide the terms for Subject Category and Subject Keyword metadata. Information management systems with a narrower application may require a more specialised terminology. Specialist terminologies can also be hosted and managed on the CVR.

---

[2] Examples of CIS of corporate interest would include, but are not restricted to, that containing personnel, personal, logistics, organisational or location information.

Definitions

14. ARD definitions are provided to support the production of glossaries and the development of CIS and help prevent conflict, confusion, or overlap and assists understanding. The use of consistent and coherent definitions will aid interoperability by enabling CIS developers to build systems that exchange information using an agreed vocabulary, and ensuring that different parts of MOD are talking the same language.

15. For example the term "Tank" is widely used across MOD and can have many different meanings. This potential incoherence can by mitigated by agreeing definitions through a Community of Interest. So in this example "Tank" would not be acceptable as an object of ARD and would be expressed instead by the contextual variations of "Tank" including "Land Vehicle Tank Combat" to denote an armoured fighting land vehicle.

16. Where a definition is designed to support CIS development then additional data will be captured. For example 'Person Unique Identifier Name' is defined as 'A unique recognisable name associated with a Person Unique Identifier' with a Data Type of 'Character' and a Length of '20'. Systems designers will use this information to ensure that any requirement involving PUID Name will be captured such that the field will be 20 characters long.

17. Definitions MUST be as brief as possible, preferably written in a single sentence, and contain only that information which makes the concept unique. MOD definitions are not meant to include everything and MUST NOT contain doctrinal information such as explanations of procedures or organisations. Information which is not essential but which may be useful to the reader may exceptionally be added in a note.

List of Values (LoV)

18. The purpose of a List of Values is to provide a selection of values for users to choose from rather than create their own. For example there are internationally agreed standards for the codes to identify countries and adherence to this will ensure consistent use of country code data across national and international boundaries.

19. Using ARD Lists of Values enables interoperability of data, uniformity in management information and helps reduce the creation of competing lists to perform a similar function. It also saves the time and money associated with the creation and maintenance of new lists.

XML Schema

20. XML schemas allow developers to specify the structure of XML documents and the data types of the information within the documents. An XML schema can indicate, for example, that a stocktaking report MUST include StockNumber, MAY include ReasonForDiscrepancyCode but MUST NOT include RequiredDeliveryDate. The schema will also provide additional information such as the required order of the tagged information and, for example, that the stock number must be in a specific format (eg NATO Stock Number format).

21. A schema can be used as part of a specification for an XML document. XML documents can also be validated against a schema to check that it meets the constraints defined in the schema. The CVR holds schema fragments that can be reused within many different schemas. For further information on MOD use of XML and XML Schemas please refer to JSP 329 Chapter 3 Annex B.

Supporting External Documents/Relevant Links:

The following publications and documents have been consulted:

- MOD Information Strategy (MODIS)

- UK Defence Terminology Guidance
- CVR
- CVR Document Store (including User Guide and other useful documents)

Contacts for this Policy

22. For guidance on applicability and implementation please email the CVR Contact Us facility or Tel: 01793 555181 or Mil 96381 5181. For more general policy enquiries please contact the CIO Information Coherence Policy team Tel: 01793 555433 or Mil 96381 5433.

MINISTRY OF DEFENCE

JSP 329 Chapter 3
MOD Electronic Data Exchange Policy

Introduction

1. MOD Policy on Electronic Data Exchange was initially disseminated by DG Info (now CIO) in Nov 06 and forms the basis of this chapter of JSP 329, which now supersedes all previous versions of the Policy.

2. The need for interoperability between Communications and Information Systems (CIS) is established as an essential requirement to facilitate information sharing across the whole of Defence, in both the operational and non operational environments, in support of Network Enabled Capability (NEC). NEC is at the heart of the transformation of Defence to support future operations and is fully described in JSP 777.

3. The use of standards to exchange information is an essential step towards achieving application interoperability and promoting information sharing between applications, both internally within the MOD and externally with partner organisations.

4. Historically, the lack of a strong governance regime to control information exchange centrally has promoted the proliferation of stove-piped application interfaces across UK Defence. Consequently, each application has demonstrated variable compliance with MOD-wide policy. This is particularly so in information exchange. Each project presently creates and maintains information exchange mechanisms to deliver its own business benefits. This means that valuable resources are being wasted, and services are being duplicated, each time a project repeats work that has already been done elsewhere.

5. When applications interoperate it is essential that the meaning of the data to be exchanged is clearly understood. This is fundamental to ensuring that the correct data is exchanged and that receiving applications can recognise and use it.

Terms and Definitions

6. Throughout this policy the following terms and definitions are used.

System	A set of software and facilities to provide business functionality to an identifiable set of users.
Open Standard	A published document that contains a technical specification, precise criteria designed to be used consistently as a rule, guideline, or definition, where such use is not subject to patent or licensing issues.

Interface	A point where two applications interact.

Policy

7. Data to be exchanged and ICS exchange mechanisms MUST be defined according to agreed and recognised[1] open standards (a hierarchical list of Preferred Open Standards can be found in Annex A). Where no appropriate Open Standard exists, data and exchange mechanisms MUST be defined in MOD compliant XML. The MOD policy on how XML is to be used in Defence is detailed in Annex B.

8. All data definitions used in information exchange, including XML definitions and schemas, MUST be recorded in the Controlled Values Repository (CVR).

9. The whole life cost of interfaces compliant with this policy MUST be part of the investment appraisal, the project plan, and the Through-Life Management Plan.

10. Existing (legacy) applications when planning upgrades or replacement MUST provide open standard or MOD compliant XML interfaces in accordance with paragraph 7 above.

11. New applications using open standards to exchange information SHOULD provide a capability to exchange information in MOD compliant XML in order to aid interoperability in the future.

12. New or upgrading systems not currently intending to interface with other applications SHOULD still provide a MOD compliant XML interface in order to aid interoperability in the future. New projects, or those planning upgrade or replacement, that cannot comply with this policy MUST contact the JSP600 (MOD CIS Policy & Assurance Process) Help Desk on 0117 91 34034 or Mil 9352 34034

13. Applications using open standard XML MUST comply with the MOD XML Header format as defined in JSP 329 Chapter 3 Annex B Appendix 1.

Reason for Implementation

14. The purpose of the Policy is to:

    a. Improve consistency of interfaces across MOD CIS by adopting the use of open standards.

    b. Promote best practice by challenging the use of non-compliant information exchange mechanisms and enable a consistent approach to interfaces.

    c. Enable greater interoperability by applying a consistent, manageable and affordable approach to data interoperability issues.

[1] Paragraph 3 of Annex A explains how the standards will be agreed and recognised.

Applicability

15. This Policy applies to all application to application data exchange within MOD and with its direct partners. It applies to new acquisition and existing applications that have, or are building, interfaces. It is intended for all staff responsible for UK Defence projects or for framing and/or implementing information strategies within MOD, who MUST comply with this Policy. It especially applies to staff and contractors responsible for the creation of applications within MOD.

Compliance Criteria

16. Projects are to provide evidence that the Electronic Data Exchange Policy is referenced in their User Requirement Document (URD) as either constraints or requirements at Initial Gate.

17. Projects are to provide evidence within their System Requirements Document (SRD) that the solution complies with the MOD Electronic Data Exchange Policy by Main Gate.

Supporting External Documents/Relevant Links:

- JSP 777 Network Enabled Capability
- JSP 600 MOD CIS Policy & Assurance Process
- JSP 602 Directory Services
- JSP 457 Vol 4 X 500 Electronic Directory Services
- MOD Metadata Standard

Contacts for this Policy

For further information on this Policy, please contact the CIO Information Coherence Policy team Tel: 01793 555433 or Mil 96381 5433.

MINISTRY OF DEFENCE

JSP 329 Chapter 3 Annex A
Standards Hierarchy

1. When selecting a standard for use across Communications and Information Systems (CIS) it is to be chosen on the basis of it having the widest acceptance, therefore the preferred option should always be an Open Standard. If a suitable Open Standard is not available the second choice should be a NATO standard, failing this select a British Standards Institute Standard. If none of these are suitable a Government Standard should be used. In certain circumstances it may be that a proprietary standard is the most appropriate to be used and possibly further developed in an MOD application. The choice of a proprietary standard must be agreed with the CIO Information Coherence Policy team.

2. The table below shows the hierarchy which must be used when selecting a suitable standard.

Preferred Standard	Open Standards including International Standards
2nd choice	NATO Standards
3rd choice	British Standards Institute Standards
4th choice	Government Standards including Defence Standards and electronic-Government Interoperability Framework (e-GIF) Standards
5th choice	Proprietary Standards

3. Within each Community of Interest (COI) there will be a preferred hierarchy of Open Standards bodies to adhere to. Although there is only one International Organization for Standardisation (ISO), there are many internationally recognised organisations and bodies working towards improved interoperability. One example of a standards body is the Open Geospatial Consortium Inc. (OGC) which is a non-profit making, international, voluntary consensus standards organisation. It can rapidly fund, invest and lead in trialing future innovation and services using its test beds within the Geospatial Environment in a more targeted and expedient manner than ISO can move in.

4. When looking for a standard to adhere to, the implementer should also look at the suitability of existing profiles of these standards. All profiles should point back to an existing recognised standard. For example Digital Geospatial Information Working Group (DGIWG) Metadata profile is a subset (with possible extensions) of the ISO 19115 Geospatial Metadata standard. DGIWG Member Nations voted to approve the profile to create it as a DGIWG standard; this

profile should be considered first in its entirety. Only if it does not meet all the requirements should the implementer refer back to the original standard. Note that ISO standards are civilian standards and may need a more restricting profile if adopted within the MOD environment.

5. Most NATO Standardisation Agreements (STANAGs) refer back to a recognised Civilian Standards Organisation or a Military Standards body and are ratified by NATO for use by all Member Nations. The STANAG agreement is in place to aid interoperability between NATO Nations and Partners. A STANAG's relevance should also be considered to aid both coherence and interoperability of an information system.

6. The British Standards Institution (BSI) is the body recognised by the UK Government for the preparation, publication and maintenance of national standards. The Government seeks to ensure that its representatives participate fully in activities at every level of BSI's Standards Board, Sector Board and Technical Committee structure. MOD is represented at senior level through the Director of Standardisation. Many of the MOD COIs will be represented on their community's relevant BSI Technical Committees, for example the Intelligence Collection Group is the voting representative on the BSI IST/036 Geographic Information Committee. BSI looks to profile and harmonise relevant standards through international, regional (European) standards organisations creating a series of publications which address the British requirements.

7. At the lowest level of the hierarchy, there may already be an approved MOD profile of an ISO standard which could be used within MOD systems to improve interoperability and coherence. These may be contained within Defence Standards, JSPs, DINs and/or e-GIF.

8. Although the examples above are related to the Geospatial COI, the underpinning principles will be the same within each COI. Careful monitoring of all the relevant standards organisations and mapping the requirements to the most relevant standard is required.

9. Standards recognised under this policy are held in a spreadsheet which can be accessed via the link below. The spreadsheet is provided as a guide and should not be viewed as an authoritative list; some standards in the spreadsheet have been superseded and before using any standard, advice should always be sought from either the CIO Information Coherence Policy team or a subject matter expert within the appropriate COI (eg DI ICSP for Geospatial standards, DSTAN for acquisition standards, etc) .

10. Against each standard in the spreadsheet will be a web link to the source for that standard. This is to ensure that up-to-date information concerning the standard can be viewed by users.

Recognised Standards Spreadsheet (Covering Restricted)

MINISTRY OF DEFENCE

JSP 329 Chapter 3 Annex B
MOD Policy on the Use of eXtensible Markup Language (XML)

Introduction

1. MOD Policy on the Use of XML was first disseminated by DG Info (now CIO) in Nov 06[1] and this Policy forms the basis of this Annex B. eXtensible Mark-up Language[2] (XML) is the MOD's preferred mechanism for passing data between disparate systems.

2. XML is an open standard which is supported by a growing body of software applications and expertise, with commitment from major suppliers. It is widely used, widely understood, and provides a mechanism to exchange information between loosely coupled computer systems. It allows different implementations to pass information in a common and neutral form.

3. XML is a method of tagging data that is widely accepted throughout industry and governments. It allows data to be defined in a consistent, clear way, independent of the implementation of the system holding the data, thus supporting structured data exchange between applications.

The Policy

4. The Policy and rules for the production of MOD compliant XML and XML Schemas are detailed in Appendices 1 to 14. A general overview of XML, describing basic terminology and reasons why we use it, is included in Appendix 15 with Acronyms and References at Appendices 16 and 17 respectively.

Appendix 1	XML Schema Document (XSD) Structure
Appendix 2	General XML Rules
Appendix 3	Namespaces
Appendix 4	Naming
Appendix 5	Attributes
Appendix 6	The Use of Instance Document Attributes
Appendix 7	Encyclopaedic Data
Appendix 8	Character Encoding
Appendix 9	The Use of Schema Elements
Appendix 10	Primitive Types
Appendix 11	Use of Mobile Code

[1] DG Info/CDMA/06-06-06 MOD Policy on the Use of XML
[2] Extensible Markup Language (XML) 1.0 (Second Edition): http://www.w3.org/TR/REC-xml

Compliance Criteria

5. The whole life cost to projects of using MOD compliant XML and XML schemas MUST be part of the investment appraisal, the project plan, and the Through-Life Management Plan.

6 New projects, or those planning upgrade or replacement, that cannot comply with this policy MUST contact the JSP 600 Help Desk on 0117 91 34034 or (9) 352 34034.

Reasons for Implementation

7. This document has been developed to provide the MOD XML developer with a framework for a consistent approach to XML and XML schema development and guidance that will standardise XML across the MOD. It also aims to promote the re-use of schema components and to aid system interoperability.

8. A set of naming and design rules is necessary because many different development options are available for designing XML documents and schemas. Further, there are many different approaches to validating particular documents against the agreed schema. As a result, without a standard, a developer in one department would generate XML documents which will not be compatible with those of another developer, even though both are using valid W3C XML. By publishing a comprehensive set of naming and design rules, the MOD aims to eliminate the potential for XML incompatibility.

9. This Policy lays down the rules for MOD compliant XML and states that schemas and XML definitions MUST be recorded and gain approval through the Controlled Values Repository (CVR) process. It should ensure that MOD compliant XML is used in a consistent manner across UK Defence to enable and support interoperability.

Applicability

10. This Policy covers all MOD compliant XML and MOD compliant XML schemas. It is applicable to all UK Defence, including all commercial and government off-the-shelf product implementation.

11. This Policy does not cover the use of XML conformant to open standard schemas, such as Geographic Markup Language (GML), Web Service Description Language (WSDL), and e-Business eXtensible Markup Language (ebXML). Where such

standards are used by MOD systems, the XML shall be structured according to that standard and use of the standard shall be registered in the CVR.

12. The MOD XML Policy is sufficiently broad to incorporate a wide variety of XML uses. Rules are primarily aimed at supporting data interchange. The rules do not, however, address the creation of XML that is used solely within a single application to carry technical (rather than business or mission execution) information pertinent only to the internal functioning of the application.

13. Human Oriented XML documents for example eXtensible HyperText Mark-up Language (XHTML), Word ML (a markup vocabulary representing content and details of Microsoft Word documents) and Open Document Format (ODF) are excluded.

14. All staff responsible for UK Defence projects or for framing and/or implementing information strategies within MOD MUST be made aware of this Policy. Those developing XML schemas and definitions MUST comply with the Policy. It especially applies to staff and contractors responsible for the specification and development of applications within UK Defence.

Requirement Classification

15. The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document, when in upper case, are to be interpreted as described in request for comments (RFC) 2119. http://www.ietf.org/rfc/rfc2119.txt

Supporting External Documentation/Related links

- NATO Guidance for XML Naming and Design document[3]
- W3c XML Schema Part 1[4] & 2[5]
- UN/CEFACT XML Naming and Design Rules Draft 1.1
- Configuration Management Plan for XML Registration and Namespaces within NATO Draft 0.6

[3] [Note re the relationship between NATO, DoD and US Dept of Navy documents]
[4] W3c XML Schema Part 1 Structures (Second Edition): http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/
[5] W3c XML Schema Part 2 Datatypes (second Edition); http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/

Appendix 1 to Chapter 3 Annex B: **Back**

XML Schema Document (XSD) Structure

1. All MOD XSD documents MUST be in two parts, the XML header and the XML body. XML instance documents (describing the data to be validated) must therefore be constructed in the same manner.

2. The XML header contains metadata, such as protective marking and document identification, some of which is mandatory. The XML header complies with the e-Government Metadata Standard (eGMS) (see eGMS Version 3.1 29 August 2006 but protective marking information is made mandatory rather than optional (see para. 4 below).

3. The Mandatory and recommended elements from the eGMS are as follows:

Mandatory Elements	**Mandatory if applicable**	**Recommended**
Creator	Accessibility	Coverage
Date	Identifier	Language
Subject	Publisher	
Title		

The full definition of these elements is provided in the eGMS.

4. The additional **Mandatory** element required by the MOD XML policy is:

Rights – specifically Protective Marking.

The full definition of the Rights element is provided in the eGMS.

5. In certain circumstances individual elements may have to have their own protective marking to allow the transition to NEC and JSP 777. To satisfy the requirement that an individual element has to have its own protective marking, the protective marking MAY be implemented as an attribute of the element in question.

6. The overhead of metadata can be reduced by implementing a single XML Header containing the metadata for all relevant XML resources, provided that the metadata is identical for all of those resources. One method of enabling this that is eGMS and Dublin Core compliant (see Guidelines for Implementing Dublin Core in XML) is as follows:

6.1 An XML Header is created which contains the mandatory metadata elements plus any required by the specific application. In this case, the mandatory if applicable Identifier metadata element is required and so is mandated.

6.2 The Identifier element is repeated in the XML Header once for each XML resource to which the XML Header refers. The Identifier element value will be the URI of each XML resource. This results in a single XML Header containing a single iteration of metadata elements such as Creator, Date, etc, but with as many iterations of the Identifier element as there are XML resources (in this case separate XML bodies) to be referenced by the metadata. Thus, there is a single XML Header containing the metadata and multiple XML body files which do not contain metadata.

6.3 It is the responsibility of the developers and owners to ensure that the intended design supports resource discovery and records management. The XML resource must therefore be linked by the Identifier (i.e. the URI) to a full set of metadata for the resource.

7. The XML body contains the approved business information.

8. The following declaration using the 'xs' prefix MUST be included: xmlns:xs="http://www.w3.org/2001/XMLSchema". This indicates that the elements and data types used in the XSD come from the "http://www.w3.org/2001/XMLSchema" namespace. It also means that the elements and data types from this namespace must be prefixed with 'xs:', e.g. 'xs:complexType'.

9. The elementFormDefault attribute MUST be declared and its value set to "qualified". This indicates that any elements from the XML instance document that were declared in this schema must be namespace qualified.

10. The attributeFormDefault attribute MUST be declared and its value set to "unqualified". This means that any attributes defined will not be attached to elements from other namespaces.

Example:

<xs:schema xmlns:xs=http://www.w3.org/2001/XMLSchema
targetNamespace=" ... see **Appendix 3** for example of Namespace... "
elementFormDefault="qualified" attributeFormDefault="unqualified">

11. Each XSD MUST have some annotation providing metadata for the document. This information MUST use the xs:documentation sub-element of the xs:annotation element rather than XML comments. The annotation MUST include the original author, a description and an update record. Each item in the update record MUST include an amendment number, the date the amendment was made, who made it and a description/comment of the amendment.
Having common metadata aids understanding, and hence correct use, of the schema. Using the xs:documentation element allows this information to be read programmatically, thereby allowing automatic documentation generation from the XSD.

Example:

```
<xs:annotation>
    <xs:documentation>
        <DC:Creator>ICAD99: John Smith</DC:Creator>
    <DC:Description>This schema contains all the … </DC:Description>
        <DC:DateIssued>2006-09-20</DC:DateIssued>
        <mod:UpdateRecord>
            <eGMS:Status version=”1”/>
            <DC:DateModified>2006-10-04</DC:DateModified>
            <DC:Contributor>ICAD99: John Smith</DC:Contributor>
    <DC:Description>Achieve validity according to XML Spy</DC:Description>
        </mod:UpdateRecord>
        <mod:UpdateRecord>
            <eGMS:Status version=”2”/>
            <DC:DateModified>2006-10-11</DC:DateModified>
            <DC:Contributor>ICAD69: Paul Jones</DC:Contributor>
    <DC:Description>Update definitions, incorporated … </DC:Description>
        </mod:UpdateRecord>
    </xs:documentation>
</xs:annotation>
```

12. Declarations of data types and globally-defined elements MUST include annotations (xs:annotation and xs:documentation) describing the meaning of the data structure. This helps understanding of the meaning of the data type or element.

Example

```
<xs:complexType name=”ComponentStructure” final=”#all” id=”331”>
<xs:annotation>
<xs:documentation>A part or combination of parts..</xs:documentation>
</xs:annotation>
……
</xs:complexType>
```

13. Although the MOD schema annotation is necessary, its volume results in a considerable increase in the size of the MOD XSD, with possible undesirable performance impacts. To address this issue it can be processed using an XSLT stylesheet that facilitates the removal of annotation when used at run-time.

14. For example, an XSLT stylesheet can be developed which is used to read in an XML file and then write out that file with the annotations removed. Other size reducing operations can be performed at the same time by the XSLT stylesheet if necessary, for example, removing any attributes which are set to default values. The <xsl:template match =”xxxx”> test condition can be used to identify the relevant artefacts. They can then be copied or not to the output file as appropriate.

15. The XSLT stylesheet can be applied at run-time or through pre-processing using an XSLT processor to create the reduced size output file.

Back

Appendix 2 to Chapter 3 Annex B:

General XML Rules

1. An existing MOD data type definition that does not meet exact requirements MAY be modified using the XML schema derivation, or inheritance, mechanism to define a new data type based largely on an existing one.
2. These modifications MAY include extension (adding new information to an existing type) or restriction (limiting the set of information allowed to a subset of that permitted by the existing type).
3. Complex type extension or restriction MAY be used where appropriate.
4. The absence of a construct or data MUST NOT carry meaning.

xs:substitutionGroup

5. The xs:substitutionGroups feature MUST NOT be used.
6. The substitutionGroups mechanism allows elements to be substituted for other elements. More specifically, elements can be assigned to a special group of elements that are said to be substitutable for a particular named element called the head element. However, there are issues with authentication, non-repudiation, ease of understanding and tool support surrounding substitutionGroups which renders it unsuitable for use.
7. All element declarations SHOULD be local except for a root element that must be declared globally. The exception is on the requirements of a community of interest, where the element is expected to be reused by the community of interest and therefore a global element declaration is appropriate.
8. Empty elements MUST NOT be used.
9. Data type definitions MUST NOT duplicate the functionality of an existing data type definition. This supports interoperability by ensuring that existing items defined with their semantics are used where possible.
10. The final attribute is only allowed to prevent further restriction or extension on xs:complexTypes that are already derived from restriction.
11. The final attribute MUST be used to control extensions.
12. The final attribute MUST be used on xs:complexType definitions derived by restriction to prevent further restriction or extensions.

13. Recursion of xs:sequence and/or xs:choice MUST NOT occur.

14. No complex type may contain a sequence followed by another sequence or a choice followed by another choice. However, it is permissible to alternate sequence and choice as in this example.

Example: xs:sequence within xs:complexType

```
<xs:complexType name="AccountType" >
<xs:annotation> ...annotation  reference e.g. Para 11... </xs:annotation>
<xs:sequence>
<xs:element name="ID" type="IdentifierType"  minOccurs="0"
      maxOccurs="unbounded"/>
<xs:element name="Status" type="StatusType" minOccurs="0"
      maxOccurs="unbounded"/>
<xs:element name="Name" type="NameType" minOccurs="0"
      maxOccurs="unbounded"/>
...
</xs:sequence>
</xs:complexType>
```

Example: xs:choice within xs:complexType

```
<xs:complexType name="LocationType">
<xs:annotation> ... annotation reference e.g. Para 11 ... </xs:annotation>
<xs:choice>
<xs:element name="GeoCoordinate" type="GeoCoordinateType" minOccurs="0"/>
<xs:element name="Address" type="AddressType" minOccurs="0"/>
<xs:element name="Location" type="LocationType" minOccurs="0"/>
</xs:choice>
</xs:complexType>
```

Example: xs:sequence + xs:choice within xs:complexType

```
<xs:complexType name="PeriodType">
...
<xs:sequence>
<xs:element name="DurationDateTime" type="DurationDateTimeType"
      minOccurs="0"/>...
...
<xs:choice>
<xs:sequence>
<xs:element name="StartTime" type="TimeType" minOccurs="0"/>
...
<xs:element name="EndTime" type="TimeType" minOccurs="0"/>
```

```
...
</xs:sequence>
<xs:sequence>
<xs:element name="StartDate" type="DateType" minOccurs="0"/>
...
<xs:element name="EndDate" type="DateType" minOccurs="0"/>
...
</xs:sequence>
<xs:sequence>
<xs:element name="StartDateTime" type="DateTimeType" minOccurs="0"/>
...
<xs:element name="EndDateTime" type="DateTimeType" minOccurs="0"/>
...
</xs:sequence>
</xs:choice>
</xs:sequence>
</xs:complexType>
```

15. Mixed content MUST NOT be used except where contained in an xs:documentation element.

16. Including mixed content in business documents is undesirable because business transactions are based on exchange of discrete pieces of data that must be clearly unambiguous. The white space aspects of mixed content make processing unnecessarily difficult and add a layer of complexity not desirable in business exchanges.

Appendix 3 to Chapter 3 Annex B: **Back**

Namespaces

1. Namespaces MUST be declared within the CVR and go through the appropriate approvals process, see the CVR Approvals Process. The prefix, URI (Uniform Resource Identifier) and a description MUST be recorded.

2. All MOD schema constructs MUST contain the xs:schema element namespace declaration using the xs: prefix:
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"> (as described in Appendix 1).

3. Every MOD schema MUST declare a target namespace using the targetNamespace attribute. The default namespace MUST be the same as this target namespace, as there is no disadvantage to this approach whereas any other approach can cause problems if another schema document is included in it.

4. A schema MAY have more than one declared namespace, but only one designated target namespace. A target namespace is declared using the namespace identifier of the selected namespace. In this example, the "http:// www.mod.uk/deas" namespace is declared as the target and default namespace:

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:deas="http://www.mod.uk/deas" targetNamespace=http://www.mod.uk/deas" elementFormDefault="qualified" attributeFormDefault="unqualified">

   Therefore any element, attribute, or data type declared in this schema belongs to the schema's target namespace.

5. The MOD has decided that URIs SHOULD be resolvable URLs (Uniform Resource Locators). Each namespace URL should, if possible, point to a location where more information about the schema can be found; although this is not mandatory as the primary purpose of assigning a URL is to provide a unique reference identifier for the namespace. This method is used by the W3C for its own schemas and is allowed in the UK Government guidelines.

6. NATO and the US have adopted the URN (Uniform Resource Name) as their standard for URIs. This is a reference that conforms to the Internet Engineering Task Force (IETF) RFC 2396, Uniform Resource Identifiers: Generic Syntax.

Appendix 4 to Chapter 3 Annex B: Back

Naming

1. Released schema documents MUST indicate their full version number in the file name as <filename>-vn-m.xsd, where n and m are the major and minor version numbers respectively and v is the character "v". Draft schema documents MUST also include their version letter as <filename>-vn-ma.xsd where “a” is the version letter of the draft.

2. If a schema document is on an annual (or other) cycle, the filename MAY incorporate a date code as well. If used, the date code MUST be included as a four character ccyy code or a six character ccyymm code.

3. MOD XML elements, attributes and types MUST be named in a consistent manner as specified below.

4. Use of a consistent naming standard helps understanding of the schemas and XML documents conforming to them.

5. The names of complex data types SHOULD end with the text string Structure. The names of simple data types SHOULD end with the text string Type. Because of this, these endings should be avoided for element names.

6. The XML name SHOULD describe the data unambiguously.

7. The XML name SHOULD be based on the content or property being described, not on its location within a particular system or model.

8. MOD XML element, attribute, and type names SHOULD be in singular form unless the concept itself is plural (example: goods)

9. In rare cases, plural names MAY be used, but the developer should use discretion to determine which XML component names are plural.

Example: <Targets>
<Target>…</Target>
<Target>…</Target>
</Targets>

Example:

Allowed - Singular: <xs:element name=”ItemQuantity” ...>
Not Allowed - Plural: <xs:element name=”ItemsQuantity” ...>

10. XML is case sensitive. Consistency in the use of case for a specific XML component (element, attribute, type) is essential to ensure every occurrence of a component is treated as the same. This is especially true in a business-based data-centric environment. Additionally, the use of visualization mechanisms such as capitalization techniques assist in ease of readability and ensure consistency in application and semantic clarity. Following the ebXML Architecture Specification and commonly used best practice, Lower Camel Case is used for naming attributes and Upper Camel Case is used for naming elements and types. Lower Camel Case capitalizes the first character of each word except the first word and compounds the name. Upper Camel Case capitalizes the first character of each word and compounds the name.

Note: These naming conventions differ slightly from the e-GSG.

11. The UpperCamelCase convention MUST be used for naming elements and types.

Example: <xs:element name="LanguageCode" ...>
Example: <xs:complexType name="DespatchAdviceCodeType">

12. The lowerCamelCase convention MUST be used for naming attributes.

Example: <xs:attribute name="unitCode" .../>

13. MOD XML Element, attribute and type names MUST be composed from words in the English language, using the primary English spellings provided in the Concise Oxford English Dictionary[1].

14. NATO and the US disallow the use of numbers, periods, spaces, and other separators, in addition to other characters not allowed by W3C XML 1.0 for XML Names, and best practice agrees with this. The MOD has followed these rules but has decided to allow numerical characters which are not disallowed by the W3C. Numerical values SHOULD not be used as the first character.

15. Acronyms and abbreviations impact on semantic interoperability, and SHOULD NOT be used.

16. Acronyms and abbreviations used MUST be recorded in the CVR.

[1] Concise Oxford English Dictionary is the basic authority used by both NATO and MOD for the meaning of English words – JSP 101

17. Once an acronym or abbreviation has been approved, it is essential to ensuring semantic clarity and interoperability that the acronym or abbreviation MUST always be used.

18. Acronyms and abbreviations at the beginning of an attribute declaration MUST appear in all lower case. All other acronym and abbreviation usage in an attribute declaration MUST appear in upper case.

19. Acronyms MUST appear in all upper case for all element declarations and type definitions.

20. Allowed – ID is an approved abbreviation

<xs:attribute name="currencyID" ….>

21. Not Allowed – Cd is not an approved abbreviation. However, if it was an approved abbreviation it must appear in all upper case as shown in the previous example.

Appendix 5 to Chapter 3 Annex B:

Back

Attributes

1. Schemas MUST be designed so that elements are the main holders of information content in the XML instances. Attributes are more suited to holding ancillary metadata.

2. XML attributes provide an alternative means to express information, but unlike elements, they cannot hold structured data. The choice between elements and attributes is a design decision with no universally accepted best practice. The MOD has chosen to adopt the principle that attributes SHOULD be used only to express metadata about business or mission execution data carried as elements. This principle minimizes attribute usage and has several desirable advantages:

   - It harmonizes the MOD approach with that of major XML business standard efforts.

   - It ensures compliance of the MOD approach with the requirements of the e-Gif.

   - It ensures that MOD XML has a consistent element/attribute structure.

Appendix 6 to Chapter 3 Annex B: Back

The Use of Instance Document Attributes

1. Null values MUST NOT be used. xsi:nil is used to differentiate between zero-length strings, zero values and undefined values. Elements that carry null values can cause XML processor errors because the database source may be expecting an integer as defined by the element type. To mitigate this type of error, the rule below is applied.

2. The xs built-in nillable attribute MUST NOT be used.

3. In general, the absence of an element in an XML schema does not have any particular meaning - it may indicate that the information is unknown, or not applicable, or the element may be absent for some other reason. The XML schema specification does however provide a feature, the nillable attribute, whereby an element may be transferred with no content, but still use its attributes and thus carry semantic meaning. However, this reduces semantic clarity.

4. The xsi:nillable attribute MUST NOT be used.

5. Each xs:schemaLocation attribute declaration MUST contain a system resolvable URL referencing the location of the schema or schema module in the release package.

6. Schema documents stored centrally SHOULD use absolute references to maintain the relationships.

7. The “xsi” prefix SHOULD be used where appropriate for referencing xsi:schemaLocation and xsi:noNamespaceLocation attributes in instance documents.

Appendix 7 to Chapter 3 Annex B: Back

Encyclopaedic Data

1. All lists of encyclopaedic data used MUST be recorded in the CVR in accordance with the requirements of JSP 329 Chapter 3 Corporate Reference Information Policy.

2. Where possible existing lists of encyclopaedic data SHOULD be used.

3. Where there is no existing list a new list SHOULD be constructed from the source data.

4. In all cases, a subset of a list MAY be used to restrict the values allowed or improve performance.

5. Universal Business Language (UBL) is the product of an international effort to define a royalty-free library of standard electronic XML business documents such as purchase orders and invoices. Developed in an open and accountable OASIS Technical Committee with participation from a variety of industry data standards organisations, UBL is designed to plug directly into existing business, legal, auditing, and records management practices, eliminating the re-keying of data in existing fax- and paper-based supply chains and providing an entry point into electronic commerce for small and medium-sized businesses. UBL XML business documents SHOULD be used where they are suitable, in preference to creating new documents.

6. The UBL format for code lists is being widely adopted throughout industry and government. Many lists, such as country codes, currency codes and units of measure, are available in this format, and others are being developed all the time. Use of this format therefore aids interoperability. UBL code lists SHOULD be used where they are suitable, and recorded in the CVR, in preference to creating new code lists.

Appendix 8 to Chapter 3 Annex B: Back

Character Encoding

1. All MOD XML documents MUST identify their character encoding within the XML declaration, except when using encryption.

2. XML supports a wide variety of character encoding. Processors must understand which character encoding is employed in each XML document. XML 1.0 supports a default value of UTF-8 (Unicode Transformation Format) for character encoding, but best practice is to always identify the character-encoding scheme being employed.

3. Also in conformance with ISO/IETF/ITU/UNCEFACT Memorandum of Understanding Management Group (MOUMG) Resolution 01/08 (MOU/MG01n83), all MOD XML MUST be expressed using UTF-8, except when using encryption.

Example: <?xml version=”1.0” encoding=”UTF-8”?>
<Person>
<Name> John </Name>
….
</Person>

Appendix 9 to Chapter 3 Annex B: Back

The Use of Schema Elements

xs:all [1]

1. The xs:all element MUST NOT be used in data centric schema

2. The xs:all element MAY be used for document centric schema.

3. Used within a group, xs:all has the same meaning as when it is used directly under xs:complexType, except that there are no minOccurs and maxOccurs attributes and it cannot be marked as optional. The xs:all compositor requires occurrence indicators of minOccurs=0 and maxOccurs=1. The xs:all compositor allows for elements to occur in any order. The result is that in an instance document, elements can occur in any order, are always optional, and never occur more than once. Such restrictions are inconsistent with data-centric scenarios such as most of the work in the MOD.

4. Another disadvantage of xs:all is that it cannot be repeated any further. This limits the use of xs:all to the first occurrence of its set of elements. If a content model requires an element that occurs more than once, then xs:all cannot be used.

xs:annotation

5. xs:annotation and xs:documentation MUST be used.

6. xs:annotation is the top level element that specifies schema comments. xs:documentation serves as a child element within xs:annotation to describe the relevant part of a schema to another human user in comparison to xs:appinfo (machine-readable documentation).

xs:any

7. The xs:any element MUST NOT be used.

8. The xs:any element enables us to extend the XML document with elements not specified by the schema.

9. The xs:anyAttribute element MUST NOT be used for data centric schema.

[1] The XML rules in this policy are based upon the Guidance for XML Naming and Design within NATO V0.4, The W3C XML Schema Part 1: Structures Second Edition and the W3C XML Schema Part 2: Datatypes Second Edition.

10. xs:anyAttribute element MAY be used for document centric schema if consistency is not an issue.

11. The xs:anyAttribute element enables us to extend the XML document with attributes not specified by the schema.

12. The any content model is the default content model when declaring an element in an XML Schema, which means that element can contain any text, white space, and child elements. In XML schemas it is known as xs:anyType. This is declared in the form:

Example: xs:anyType

<xs:element name = “myElement” type = xs:anyType”/>
But as it is the default, this would be equivalent to:
<xs:element name = “myElement”/>

Generally the use of xs:anyType can be helpful at the start of a schema development, but the use has to be restricted and the schema tightened down as soon as possible to avoid errors creeping in.

xs:appinfo

13. The MOD recommends that developers SHOULD NOT use xs:appinfo or put any application information within the schema.

14. If used, xs:appinfo MUST only be used to convey non-normative data.

15. The xs:appinfo element occurs within the annotation element and specifies information to be used by the application, as opposed to xs:documentation that contains human-readable information.

xs:attribute

16. Attribute declarations SHOULD only be used for expressing metadata about business or mission execution data carried as elements.

17. Attribute declarations provide for:

- Local ·validation· of attribute information item values using a simple type definition; specifying either default or fixed values for attribute information items.

- Expressing metadata about business or mission execution data carried as elements.

Example:

<xs:attribute name="age" type="xs:positiveInteger" use="required"/>
The XML representation of an attribute declaration.

xs:attributeGroup

18. The xs:attributeGroup element MAY be used.

19. The xs:attributeGroup element is used to group a set of attribute declarations so that they can be incorporated as a group into complex type definitions.

xs:attributeGroup Element Information:

20. Parent elements: attributeGroup, complexType, schema, restriction (both simpleContent and complexContent), extension (both simpleContent and complexContent)

Example:

```
<xs:attributeGroup name="personattr">
    <xs:attribute name="attr1" type="string"/>
    <xs:attribute name="attr2" type="integer"/>
</xs:attributeGroup>

<xs:complexType name="person">
    <xs:attributeGroup ref="personattr"/>
</xs:complexType>
```

This example defines an attribute group named "personattr" which is used in a complex type named "person".

xs:choice

21. The xs:choice element MAY be used.

22. The xs:choice element allows for any one, but only one, of several child elements to occur in content. Group compositors are either all, choice, or sequence.

23. Choice groups allow for more complex content models. A choice group of element declarations is used to indicate that only one of the corresponding conforming elements must appear. Analogously to xs:all this feature can be inconsistent with business transaction exchanges, but could be very useful for a construct in situations where customization and extensibility are not a concern. Despite that xs:choice cannot be extended.

xs:complexType

24. xs:complexType MAY be used.

25. Any xs:complexType derived by restriction MUST NOT be further extended.

26. xs:complexType is an XML element that contains other (sub) elements and/or attributes. It is assumed that, in many cases, in the development of new schema within the MOD domain there will be instances of reuse of schema that will need restriction to create the desired results.

xs:documentation

27. xs:documentation MAY be used.

28. xs:documentation serves as a child element within xs:annotation to describe the relevant part of a schema to another human user in comparison to xs:appinfo (machine-readable documentation).

xs:element

29. xs:element MAY be used.

30. Each XML document contains one or more elements, the boundaries of which are either delimited by *start-tags* and *end-tags*, or, for *empty* elements, by *an empty-element tag*. Each xs:element has a type, identified by name, sometimes called its "generic identifier" (GI), and may have a set of attribute specifications. Each attribute specification has a *name* and a *value*.

xs:extension

31. xs:extension MAY be used.

32. The extension element extends an existing simpleType or complexType element by adding attributes or elements to those specified within an existing type definition.

xs:field

33. xs:field MAY be used.

34. {xs:field}s specifies XPath expressions relative to each element selected by xs:selector. This must identify a single node (xs:element or xs:attribute) whose content or value, which must be of a simple type, is used in the constraint. It is

possible to specify an ordered list of {xs:field}s, to cater to multi-field keys, keyrefs, and uniqueness constraints.

xs:group

35. xs:group MAY be used.

36. The group element is used to define a group of elements to be used in xs:complexType definitions.

Example:

```
<xs:group name="myModelGroup">
      <xs:sequence>
        <xs:element ref="someThing"/>
       . . .
      </xs:sequence>
    </xs:group>

    <xs:complexType name="trivial">
      <xs:group ref="myModelGroup"/>
       <xs:attribute .../>
    </xs:complexType>

    <xs:complexType name="moreSo">
      <xs:choice>
        <xs:element ref="anotherThing"/>
        <xs:group ref="myModelGroup"/>
      </xs:choice>
     <xs:attribute .../>
    </xs:complexType>
```

A minimal model group is defined and used by reference, first as the whole content model, then as one alternative in a choice.

xs:import

37. The code list xs:import element MUST contain the namespace and schema location attributes.

38. xs:import MUST NOT be used without a namespace attribute.

39. xs:import is used to bring schema modules that reside in a different namespace into the target namespace of a master or root schema.

40. Use of xs:import without a namespace attribute allows unqualified reference to foreign components with no target namespace. This would lead to schemas which are difficult to debug and to update – and for which the reuse dependencies were invisible.

xs:include

41. The xs:include MAY only be used in a development or enterprise run-time root schema.

42. The xs:include SHOULD NOT be used for schemas other than development or enterprise run-time root schema.

43. The xs:include element is used to add multiple schemas to a document. The included schema must have a “schemaLocation” attribute with an URI pointing to a valid schema. Furthermore the included schema must define either the same or no target namespace. If the schema target namespace does not match, the xs:include will not work.

xs:key/xs:keyref

44. xs:key/xs:keyref MUST be used for information association.

45. The xs:keyref identity constraint names MUST consist of the name of the referencing object class plus the name of the referenced object class plus the suffix “REFKey.”

46. The XML Schema construct xs:keyref is used in conjunction with xs:unique to identify relationships between model elements. The name of xs:keyref constraints is constructed by concatenating the referencing object class to the referenced object class and appending the string “REFKey.”

xs:notation

47. xs:notations SHOULD NOT be used.

48. The notation element describes the format of non-XML data within an XML document. A notation in XML is just like the notation declarations in DTDs. Although xs:notation is not compatible with notations in Document Type Definitions (DTDs), because the xs:notation is a “QName”. The main difference is that W3C XML Schema notations are namespace-aware and can be imported between schemas. Notations are referenced in the course of validating strings as members of the xs:enumeration facets simple types xs:notation is used to declare the format of non-XML data. Schema notations are namespace-aware and can be imported between schemas. When these declarations are used, the notations are used in xs:enumeration facets to create simple types.

xs:redefine[2]

49. xs:redefine SHOULD NOT be used.

50. The xs:redefine element redefines simple and complex types, groups, and attribute groups from an external schema. To avoid pervasive side-effects in reused components, and to increase clarity and readability it should not be used.

xs:restriction

51. When xs:restriction is applied to a xs:simpleType or xs:complexType the derived construct MUST use a different name.

52. xs:restriction is used as appropriate to define types that are derived from the existing types. Where used, the derived types MUST always be renamed. Simple and complex type restrictions MAY be used.

xs:selector

53. xs:selector MAY be used.

54. xs:selector specifies a restricted XPath expression relative to instances of the element being declared. This identifies a node set of subordinate elements (i.e. contained within the declared element) to which the constraint applies. xs:field specifies XPath expressions relative to each element selected by a xs:selector. This identifies a single node (element or attribute) whose content or value, which is of simple type, is used in the constraint. It is possible to specify an ordered list of {fields}, to cater for multi-field keys, keyrefs, and uniqueness constraints.

xs:sequence

55. xs:sequence MAY be used.

56. In the example below notice the <xs:sequence> tag. It means that the elements defined ("firstname" and "lastname") must appear in that order inside a "person" element. Or you can give the complexType element a name, and let the "person" element have a type attribute that refers to the name of the complexType (if you use this method, several elements can refer to the same complex type).

57. You can define the "person" element in a schema, like this:

[2] This rule is derived from the e-Gif policy on XML.

Example:

```
<xs:element name="person">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="firstname" type="xs:string"/>
      <xs:element name="lastname" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
```

xs:simpleContent

58. xs:simpleContent element SHOULD contain either the xs:extension or xs:restriction element.

59. When using simple content, you MUST define an extension OR a restriction within the simpleContent element.

60. This type contains only simple content (text and attributes), therefore we add a xs:simpleContent element around the content.

Example:

```
<xs:element name="somename">
  <xs:complexType>
    <xs:simpleContent>
      <xs:extension base="basetype">
        ....
        ....
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
```

xs:simpleType

61. xs:simpleType MAY be used.

62. xs:simpleType element SHOULD contain either the xs:extension or xs:restriction element.

63. The simpleType element defines a simple type and specifies the constraints and information about the values of attributes or text-only elements.

Example:

```
<xs:simpleType name="MissionThreadType">
      <xs:annotation>
        <xs:documentation> A Mission Thread is … </xs:documentation>
      </xs:annotation>
      <xs:restriction base="xs:string" />
</xs:simpleType>
```

xs:union

64. The xs:union technique MAY be used for code lists.

65. The xs:union technique MUST NOT be used for any purpose other than code lists.

Example:

```
<xs:simpleType name=“>
        <xs:union memberTypes=“/>
</xs:simpleType>
```

xs:unique

66. xs:unique MAY be used to normalize XML instances by expressing one-to-many relationships between model classes/entities.

67. The xs:unique identity constraints names MUST be the same as the entity object class being identified uniquely plus the suffix “Key.”

68. The name of the xs:unique identity constraint is the object class name of the class/entity being identified uniquely plus the string “Key.”

Appendix 10 to Chapter 3 Annex B: Back

Primitive Types

xs:ID/IDREF

1. xs:ID/IDREF MUST NOT be used.

2. ID, IDREF and ENTITY are XMl Schema built-in datatypes derived from NCName (No-colon Name, W3C informally defined as “an XML Name minus the ‘:’).

xs:anyType

3. The xs:anyType MUST NOT be used.

The use of xs:anyType permits the introduction of potentially unknown types into XML documents. xs:anyType is seen as working counter to the requirements of interoperability.

Appendix 11 to Chapter 3 Annex B:

Back

Use of Mobile Code[1]

1. Mobile code MUST NOT be carried within an XML document unless it has a "Very Limited" risk. The acceptable languages for use at the time of writing are:

ECMAscript (including Jscript and JavaScript);
Portable Document Format; and
Shockwave / Flash.

This is in line with CESG Infosec Memorandum No. 21, Risk Management in Mobile Code.

2. Mobile code in XML, as in other environments, carries significant security risks. These MUST be controlled if the advantages of XML are to be realised. However, use of active content can greatly increase the effectiveness of systems and, within the security constraints, is therefore encouraged.

[1] Mobile code: software obtained from remote systems outside the enclave boundary, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. Source: US DoD Memorandum: Policy Guidance for use of Mobile Code Technologies in Department of Defense (DoD) Information Systems.

Appendix 12 to Chapter 3 Annex B: Back

XLST – XML Rendition and Transformation

1. XML documents do not normally include any information about their presentation. A separate style sheet is usually needed to define how the documents are to be presented.

2. eXtensible Stylesheet Language (XSL) is the main language for rendering XML documents. XSL is very flexible and is often used in conjunction with Cascading Style Sheets (CSS) to produce eXtensible HyperText Mark-up Language XHTML.

3. XSLT SHOULD be used to define the translation of XML documents from one layout to another.

4. There are two related XSL languages: eXtensible Stylesheet Language Transformation (XSLT) and eXtensible Stylesheet Language Formatting Objects (XSL-FO). XSLT defines how an XML document can be transformed. XSL-FO defines how this document should be displayed. If the target device for displaying the data in the XML document is a web browser, the target format will be XHTML. In this case, it is only necessary to use XSLT to achieve the required transformation. If the target format cannot be well-formed (e.g. when creating a PDF document from XML), XSLT is used to provide a preliminary transformation, and XSL-FO to define the document appearance.

5. Translation may be required for several reasons, such as:

   to add an MOD XML Header to an incoming document;
   to remove protectively marked material at a boundary;
   to merge XML document content from several sources to produce another document;
   to reformat an outgoing XML document to meet the requirements of external partners since different partners may use different schemas for the same purpose; or
   to reformat an incoming XML document from an external partner.

   In some of these cases the XML may be translated so that it complies with a different schema from the one for which it was originally created.

Appendix 13 to Chapter 3 Annex B: Back

Versioning

1. MOD schema components MUST be version controlled to address potential backward-compatibility issues inherent in XML processing. XML namespace and schema versioning provide the MOD with the best long-term versioning strategy because it allows the MOD developer to access the latest enterprise core components without interrupting production applications that reference an older component.

2. Definitions and schemas when they become approved in the CVR are base lined at version 1.0.

3. A MOD namespace URN is divided into three parts. First is the standard MOD namespace information. Second describes the purpose of the namespace. Third is the version information. MOD schema components must have version control, which is handled by version information, consisting of major (or incompatible) and minor (or compatible) fields. An optional revision extension may be used in addition to the minor field.

Example:

Namespace="urn:<MOD namespace information>:<purpose of namespace>:<major version>:<minor version>:[<revision>]"

[ ] denotes optional extension to the URN

4. The major or minor version number MUST be updated following changes to the definitions and schemas.

5. Minor version number updates MUST be limited to declaring new optional constructs, extending existing constructs, and refinements of an optional nature.

6. For a successful strategy, namespace versioning shall align with schema versioning and modularity, which means that version information must be contained in both the schema and in the schema's target namespace. This section will detail the MOD versioning guidelines for both namespace and schema.

7. The initial release of MOD enterprise reusable components MUST start with a 1.0 (the URN ends in "1.0"). Subsequent new components MUST be added to the 1.0 namespace by creating a new XSD in the namespace. The previous XSD is included in the new XSD so that all 1.0 components are available from it.

8. New versions of existing components MUST be added to higher versioned namespaces.

9. A new schema does not have to hold the previous version, especially if some terms have been retired or superseded. However, it will require a major version increment when introduced. On the other hand a minor version update MUST incorporate the previous major or minor versions.

10. Namespaces provide a means for achieving consistency and harmonization between schema versions. In practice this means that new components will need to be added to eg the 1.0 enterprise namespace at intervals and new versions of existing components will need to be added to higher versioned namespaces. This addition of new components to a namespace that already has components is accomplished by creating a new schema in the namespace. This new schema then includes the previous schema. In accordance with this complex process MOD expects full forward and backward compatibility.

Appendix 14 to Chapter 3 Annex B: Back

Registering XML

1. XML schemas and all related element and data type declarations MUST be agreed across MOD, recorded centrally and made available to all MOD information systems and staff.

2. The mechanism to achieve this uses the Controlled Values Repository (CVR). XML schemas and related definitions used in the MOD MUST be registered in the CVR prior to use in normal operation.

3. All XML documents produced by MOD systems MUST use Approved XML schemas, held in the CVR, and MUST conform to the standards and procedures on XML as defined in this policy document.

4. Where any user of XML in UK Defence determines a need for a schema, they MUST search the CVR for a suitable Approved schema. If no suitable schema is found they MUST search the CVR for suitable complex/simple types, which could be developed into a schema. If the schema can be built entirely of existing complex/simple types, then the new schema MUST be registered in the CVR – such schemas will have only one new complex type definition, ie for their top level.

5. Schemas that are protectively marked higher than Restricted MUST not be registered in the CVR. Instead the way forward for the schema MUST be discussed with the CVR Contact us facility.

6. All XML schema definitions used within the MOD MUST have an MOD schema owner. Changes MUST NOT be made without the approval of the schema owners. When an external schema is registered for use in the MOD, whether directly or through translation, the external owner of the schema must also be identified. The MOD Owner of an external schema SHOULD consider membership of the external body that manages the schema.

7. Defining ownership allows changes to be made in a controlled way with proper authorisation. Having the MOD owner join the appropriate external body will allow users of the schema within the MOD to have early sight of any proposed changes and to influence those changes.

8. Registration of all XML Schema and their related element and data type declarations ensures that they are agreed across MOD and its partners and are available to all MOD information systems. It further ensures that the data contained in associated instance documents can be understood and handled correctly.

9. New or amended schemas and their associated definitions MUST NOT be used until they have completed the staffing procedure.

10. When satisfied that a new schema fully meets their requirements, the schema owner or user must then submit the schema to the DBS. Using the CVR, the schema will then be staffed across all relevant Communities of Interest (COIs) within MOD for approval.

11. Namespaces MUST be registered in the CVR. New namespaces will only be established if there is an exceptional business need for a deployment of a set of schemas, which is different from any existing CVR approved namespace.

Appendix 15 to Chapter 3 Annex B: Back

Background Information on XML

What is XML?

1. The eXtensible Mark-up Language (XML) is a method of tagging data that is widely accepted throughout industry and governments. The tags used generally describe the meaning of the data and are defined by the user. For example, data on an item of equipment might contain information such as:

<StockNumber>1234567891234</StockNumber>

In this case, the text < StockNumber > is known as a start tag, the text </ StockNumber > as an end tag, the complete text between the start of the start tag and the end of the end tag as an element and 1234567891234 as the value of the element. The element is called StockNumber, which is also called the tag name and XML name. This data might be part of either a document that is to be printed (such as a stocktaking report) or a message that is to be transmitted from one database to another (for example, submitting an equipment purchase request to a manufacturer).

2. Tagging data in this way makes it easily readable by both people and computers. Although in many cases the data is both produced and consumed by computers, experience has shown that expressing the data in a human-readable format speeds development and reduces errors. The trade-off is that the mark-up adds characters to the data stream compared to, say, comma-delimited data. However, in most applications now, people find that the advantages of ease of development, ease of debugging, ready access to tools and fast development with lower costs outweigh this disadvantage. Where the size of the data stream is important, advantage can be taken of the highly compressible nature of XML.

3. XML is an open standard which is supported by a growing body of software applications and expertise, with commitment from major suppliers including Microsoft, IBM, and Sun. It is widely used, widely understood, and provides a mechanism to exchange information between loosely coupled computer systems, allowing widely differing implementations to pass information

4. XML enables data to be exchanged in a format that is neutral and unaffected by the manner in which it is to be handled at its destination. This means that an XML message can be sent to a group of recipients (including other computer systems of various types, PC users using a web browser and mail client). Each recipient uses the content of the message for their own purposes (the originator of the message does not need to be aware of its use).

5. XML allows data to be defined in a consistent, clear way, independent of the implementation of the system holding the data, thus supporting structured data exchange between applications.

6. XML is supported by a number of related software tools, applications and languages, which provide consistent methods of handling XML data – presenting, transforming, navigating, and parsing it. One of these used in this Policy is eXtensible Stylesheet Language (XSL), which can manipulate defined data in a consistent way to ensure that it is converted to and from an agreed form providing a coherent mechanism to support conversion at system boundaries.

7. Information is required to indicate the set of tags that are required and allowed in a specific type of XML document. XML schemas allow developers to specify the structure of XML documents and the data types of the information within the documents. An XML schema can indicate, for example, that a stocktaking report MUST include StockNumber, MAY include ReasonForDiscrepancyCode but MUST NOT include RequiredDeliveryDate. The schema will also provide additional information such as the required order of the tagged information and, for example, that the stock number must be in a specific format (eg NATO Stock Number format).

8. A schema can be used as part of a specification for an XML document. You can also validate an XML document against a schema to check that it meets the constraints defined in the schema.

9. A schema does not provide a complete message specification for two reasons. The first is that a schema defines structure and data types, but does not define meaning. For example a schema might define that an element called “title” contains a text string of up to 35 characters, but can give no indication of its meaning. The second reason is that the W3C Schema definition language itself has limitations. In particular, it cannot be used to define constraints across multiple pieces of information. For example, in a unit position and status report, it could not be used to indicate that, if the value of an element called “PlatformType” is “Ship”, then the element “Altitude” must be absent.

10. The CVR holds schema fragments that can be reused within many different schemas.

11. There are many different ways of creating a schema for a particular XML document. The XML policy addresses the issues that there are with this and mandates how MOD compliant XML should be created. See below for an example of an XML schema that defines the XML document also given below:

<u>An Example of XML</u>

```
<?xml version="1.0" encoding="UTF-8"?>

<AirfieldStatus>
        <StationName> Kinloss </StationName>
        <ServiceName> Royal Air Force </ServiceName>
        <Store> AIM-9L AAM</Store>
        <Store> AIM-9M AAM</Store>
        <Store> AMRAAM AAM</Store>
        <Store> Stingray Torpedo</Store>
        <Store> Sonobuoy A-Size </Store>
        <Store> Sonobuoy G-Size </Store>
        <Store> Sonobuoy F-Size </Store>
        <Store> 20 mm Ammunition </Store>
        <Store> 27 mm Ammunition </Store>
        <Store> AS Depth Charge </Store>
</AirfieldStatus>
```

An XML Schema Example

```
<?xml version="1.0" encoding="UTF-8" ?>

<?xml version="1.0" encoding="UTF-8" ?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

<xs:complexType name="AirfieldStatusStructure">
        <xs:annotation>
            <xs:documentation> Airfield status is ... </xs:documentation>
        </xs:annotation>
        <xs:sequence>
          <xs:element name="StationName" type="StationNameType" />
          <xs:element name="ServiceName" type="ServiceNameType" />
          <xs:element name="Store" type="StoreType" maxOccurs="unbounded"/>
        </xs:sequence>
</xs:complexType>

<xs:simpleType name="StationNameType">
        <xs:annotation>
            <xs:documentation> A Station Name is ... </xs:documentation>
        </xs:annotation>
        <xs:restriction base="NameType" />
</xs:simpleType>

<xs:simpleType name="ServiceNameType">
        <xs:annotation>
            <xs:documentation> A Service Name is ... </xs:documentation>
```

```
        </xs:annotation>
        <xs:restriction base="NameType" />
</xs:simpleType>

<xs:simpleType name="NameType">
        <xs:annotation>
            <xs:documentation> A Name is ... </xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:maxLength value="20" />
        </xs:restriction>
</xs:simpleType>

<xs:simpleType name="StoreType">
        <xs:annotation>
            <xs:documentation> A Store is ... </xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string" />
</xs:simpleType>

</xs:schema>
```

Why Use XML?

12. The world is full of incompatible computer systems. Within Government, many such systems have operated in isolation – for example one to collect taxes, one to calculate benefits and another to manage the judicial system – and for a long time this was not a problem. Now these systems are required to communicate with each other and with external partners, citizens and businesses.

13. To achieve a fully joined-up Government or Government Department, there are three main interoperability requirements. Documents must be held in a way that they can be published not just on paper, but also through a variety of electronic media. Information must be transferred between computer systems. And systems must be able to both provide services and request these services from each other.

14. XML handles these requirements very well and this is why XML has become the key enabling technology for e-Government in the UK, the USA and many other countries.

15. XML was designed as an industry standard for independent systems to exchange information provided they adopt a common data transfer mechanism that is neutral and unaffected by the manner in which it is to be handled at its destination. XML provides a robust, non-proprietary (open standard), verifiable

file format for the storage and transmission of text and data. Although initially targeted at Web developers the rapid adoption of XML in all IT fields within the commercial market place demonstrates that XML provides a format that is flexible enough to accommodate widely diverse needs.

16. The world's largest software companies all support XML as a key part of their product strategies. XML also provides new opportunities for smaller companies. This means that there are plenty of products in the market that can be used to help create an e-Government relatively cheaply and without the risk of a manufacturer replacing the technology after an investment in e-Government has been made.

17. XML can be used to allow existing systems to communicate with each other, rather than having to replace them. This, above all, makes XML a sustainable technology. In addition, because XML is not dependent on any technology platform, future replacements of computer systems will not require replacement of existing XML processes.

18. The e-GIF has been developed by the UK Government to specify standards to use for different applications. This helps with re-use of data definitions and ensures interoperability between systems developed for use in the UK public sector.

19. The UK Government's e-GIF directives bind the MOD, in line with all other public sector organisations, to adopt Internet and World Wide Web (WWW) specifications for interoperability between government departments. e-GIF mandates the adoption of XML and XSL as the core standards for data integration and management of presentational data.

20. The US, NATO, UK and many other governments are already active in developing XML to support Message Text Formats.

21. The UK Government, many trading standards bodies and many other governments have adopted XML as the format for exchanging information.

22. The MOD Data Interoperability Paper (approved by the Defence Information Reference Group Executive (DIRGE) on 23 June 2004), which is an integral part of the Information Exploitation (IX) initiative, promotes XML as a primary enabler of Data Interoperability in Defence. Without the use of XML the goals and benefits of Data Interoperability will not be realised. The XML Policy is therefore an essential component of the drive to deliver Information eXploitation (IX) in a Network Enabled Capability (NEC) context.

23. XML is supported by a growing body of software applications and expertise, with commitment from major suppliers including Microsoft, IBM, and Sun. It is widely used and widely understood.

24. XML is human readable, simplifying testing, faultfinding, and bug rectification.

25. Because XML uses standard off-the-shelf products for information exchange it is an effective and economical way of exchanging information.

26. XML can provide a single view of the structure of data, defining the information in use so that information which passes across system boundaries can be defined in a way which is understandable by all the parties involved.

27. XML allows data to be checked for validity against a pre-defined standard in a clear and coherent manner, wherever it occurs, especially during a data transfer. Thus greatly reducing (though not eliminating) the opportunity of passing corrupt information between systems.

28. XSL allows disparate systems (including, if resources allow, legacy systems) to pass data as XML, ie in an application-neutral, fully understood, well-documented, human readable form. XML thus supports structured data exchange between applications, independent of implementation.

29. The use of XML as the means of exchanging documents with external partners will remove many of the barriers to rapid inter-organisational transaction processing. This will enhance both the effectiveness and efficiency of the MOD and its partners so achieving the benefits envisaged for information age government.

30. XML separates content from style. This enables easier data re-use and the generation of multiple outputs from the same data. This will eliminate the waste of resources required to maintain the enormous number of individually designed and built interfaces - both those currently in place and those being developed.

<u>What are the Disadvantages of XML and how can these be overcome?</u>

31. XML is verbose: that is, it surrounds the information formatted using it with a great deal of additional information much of which is repetitive and unnecessary for computer systems. However, because of its repetitive nature, XML Documents are very compressible.

32. Uncompressed XML data is relatively predictable, which makes it slightly easier to attack any encryption.

33. However, compressed XML is highly random, which makes it more secure, and it is also shorter, which gives the attacker less data to play with for a brute force attack. Indeed, the “codebook” mechanism would offer a very significant degree of protection by itself: without matching data tables at the two ends, the compressed message is useless.

34. XML permits any user to define data: this allows multiple users to define it differently. The same item of information may be given a number of different names, or different items may be identified by the same name. The same piece of information may be specified with different formats or sets of code values. XML contains a mechanism, the “Namespace” to handle this chaos, but all it does is allow these variously defined items to be handled at the same time: it does not provide any mechanism to automatically convert between them. This is overcome by this policy.

35. In spite of a number of initiatives, such as the work at NATO to convert AdatP-3 messages to a coherent set of XML elements, there has been considerable resistance to the use of XML in some areas of the battlespace. Most objections have centred on the additional bandwidth that will be required for XML messages (not without reason, since its prolix nature will obviously have serious repercussions in a restricted-bandwidth environment).

36. However, as noted above, these bandwidth problems can be overcome by well-understood mechanisms using the excellent compressibility characteristic of XML.

Why do we need this Policy?

37. The W3C XSD (XML Schema Definition) schema was designed to be flexible enough to satisfy a diverse set of user requirements in a wide range of organisational and trading partner environments. This flexibility offers the designer many choices - global versus local elements, use of built-in simple types or creation of user-defined simple and complex types, and derivation of types and elements by extension or restriction, to name but a few. However, this flexibility has certain drawbacks, primarily when attempting to use XML in a manner that enhances rather than detracts from interoperability, or more succinctly, when attempting to ensure consistency in XML implementations within a particular organization or enterprise.

38. The MOD views XML as a key enabler in achieving enterprise interoperability and promulgating authoritative source data. Achieving these goals using XML requires establishing rules for consistent XML schema creation by all MOD stakeholders. These rules must provide concise and clear guidance on the design and use of XML. More important, these rules must clearly articulate the which, why, and how MOD XSDs will be designed.

39. Chief among the design decisions the MOD must address is how to declare XML elements. Schema language provides many redundant features that allow a developer to represent a logical data model many different ways. Heterogeneous data models can become an interoperability problem without

prescribing a comprehensive set of naming, definition, and declaration design rules.

40. This policy establishes rules for XML schema elements, attributes, and type creation. Because the W3C XML specifications are flexible, the MOD requires comprehensive rules to achieve a balance between establishing uniform schema design while still providing developers flexibility across the MOD.

41. It is essential that the format of XML documents can be understood by all users and can be validated by document recipients. This facility is provided by the XML Schema language.

42. The purpose of the Policy is to ensure consistent interfaces across MOD by mandating the use of XML to MOD Standards. The Policy mandates that MOD Data is defined in a common way, so that it can flow freely across the MOD Domain. This will support NEC, by allowing the use of web-enabled technologies to support the agile use of MOD information wherever held and wherever required, in a properly controlled environment.

43. The effect of this is to ensure that XML in MOD is developed in a coherent manner, thus ensuring consistent use of data and allowing a well-understood set of supporting tools to be used.

What is a Namespace?

44. In practice, many organisations will use the same element names for different things. Clearly this happens in natural language as well. If the word "track" is used, it could mean the track of a tank, the ground track of an aircraft, or even a railway track. In most cases of natural language, we know by the context. In XML, we use namespaces.

45. A namespace in XML is simply a qualifier on a tag name to indicate ownership. This qualifier is in two parts. The first part is applied as a user defined prefix to a tag name, so StockNumber might become deas:StockNumber. The second part is only required once in every XML document or message and associates the prefix with a unique text string, which is called the Uniform Resource Identifier (URI). It is also possible to associate a string with the absence of a prefix, providing a default namespace when no prefix is used.

46. Neither XML 1.0 nor XSD require the use of Namespaces. However the use of namespaces is essential to managing a complex MOD library of definitions.

47. A namespace is declared in the root element of a schema. The declaration associates the prefix with the URI making the constructs “namespace qualified”.

48. In the following example, the namespace identifier is a URL "http://www.mod.uk/deas" and the namespace prefix is "deas":

Example:

<xs:schema xmlns:deas="http://www.mod.uk/deas">

49. Namespaces allow XML elements with the same name to be used in the same schema with no adverse effects. In the following example, two "State" elements are used in the same schema, but they are associated with two different namespaces. One element represents a U.S. state abbreviation (AK, AL, AR) in the Department of the Navy's namespace, while the other represents the state of water quality (acidic, basic, high turbidity) in the Department of the Army's namespace:

Example: Namespace Prefix Association

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:don="urn:us:gov:dod:don" xmlns:doa="urn:us:gov:dod:doa">
<xs:element name="don:State" type="don:StatePostalCodeType"/>
<xs:element name="doa:State" type="doa:WaterQualityIndicatorType"/>
</xs:schema>

If the "State" elements described above were not in separate namespaces, an XML processor would generate an error. This condition is known as "name collision."

Appendix 16 to Chapter 3 Annex B: Back

ACRONYMS

CESG	Communications Electronics Security Group
CSS	Cascading Style Sheets
CVR	Controlled Values Repository
DBS	Defence Business Services
DIRGE	Defence Information Reference Group Executive
DMG	Data Management Group
DTD	Document Type Definition
e-GSG	e-Government Steering Group
e-GIF	e-Government Interoperability Framework
ebXML	e-Business eXtensible Markup Language
GML	Geographic Mark-up Language
HTML	HyperText Mark-up Language
ICAD	Information Coherence Authority for Defence
IETF	Internet Engineering Task Force
IX	Information eXploitation
JSP	Joint Service Publication
MOD	Ministry of Defence
MOUMG	Memorandum of Understanding Management Group
NATO	North Atlantic Treaty Organization
NEC	Network Enabled Capability
OASIS	Organization for the Advancement of Structured Information Standards
ODF	Open Document Format
RFC	Request For Comments
UBL	Universal Business Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UTF	Unicode Transformation Format
WSDL	Web Service Description Language
WWW	World Wide Web
W3C	World Wide Web Consortium
XHTML	eXtensible HyperText Mark-up Language
XML	eXtensible Mark-up Language
XSD	XML Schema Definition
XSL	eXtensible Stylesheet Language
XSLT	eXtensible Stylesheet Language Transformation
XSL-FO	eXtensible Stylesheet Language Formatting Objects

Appendix 17 to Chapter 3 Annex B: **Back**

References

1. Key words for use in RFCs to Indicate Requirement Levels
   http://www.ietf.org/rfc/rfc2119.txt

2. CVR
   http://www.cvr.dii.r.mil.uk

3. eXtensible Markup Language (XML) 1.0 (Second Edition)
   http://www.w3.org/TR/REC-xml

4. The e-Government Interoperability Framework
   http://www.cabinetoffice.gov.uk/govtalk/schemasstandards/e-gif.aspx

5. XML Schema Part 1: Structures, W3C Recommendation 2001 and
   http://www.w3.org/TR/xmlschema-1/

6. XML Schema Part 2: Datatypes, W3C Recommendation 2001
   http://www.w3.org/TR/xmlschema-2/

7. XML-Signature Syntax and Processing, W3C Recommendation 2002
   http://www.w3.org/TR/xmldsig-core/

8. Universal Business Language (UBL) Code List Representation, see
   http://www.oasis-open.org/committees/sc_home.php?wg_abbrev=ubl-clsc

9. XSL Transformations (XSLT) Version 2.0
   http://www.w3.org/TR/xslt20/

10. Cascading Style Sheets, level 2: CSS2 Specification
    http://www.w3.org/TR/CSS2/

The Policy has been based on various other policies including:

W3C XML Schema Part 1: Structures Second Edition
W3C XML Schema Part 2: Datatypes Second Edition
Guidance for XML Naming and Design within NATO V 0.4
Additional documents that have been referenced:
UN/CEFACT XML Naming and Design Rules Draft 1.1
Configuration Management Plan for XML Registration and
Namespaces within NATO" Draft 0.6
E-Government Schema Guidelines for XML v3.1

MINISTRY OF DEFENCE

JSP 329 Chapter 4
MOD Metadata Policy

Introduction

1. In accordance with the mandatory pan-government directive (see supporting documents), the MOD is required to conform to the current version of the e-Government Metadata Standard (e-GMS) [e-GMS Version 3.1].

2. The e-GMS lays down the elements, refinements and encoding schemes to be used by government officers when creating metadata for their information resources or designing search interfaces for information systems. The e-GMS is needed to ensure maximum consistency of metadata across public sector organisations.

3. The MOD Metadata Standard (MMS), which meets the minimum requirements laid down in the e-GMS, has been created and agreed by key stakeholders to meet MOD's specific business requirements. Metadata (labelling information resources – refer to JSP 717 for further explanation) is primarily needed to support resource discovery and records management.

Policy

4. The MMS is mandated for Electronic Document and Record Management Systems (EDRMS), document management systems and Content Management Systems (CMS), so that every information asset created in these systems is accompanied by metadata. This metadata policy MUST be adhered to by the developers and owners of EDRMS, document management systems and CMS.

5. CIS systems SHOULD also adhere to the minimum mandatory requirements cited in the MMS, if the information is to be used, or there is a potential business use of the information beyond the domain in which it resides.

6. A full list of metadata fields for all types of information asset is given in the standard, however not all of the fields are mandatory for every information resource, and these parts of the standard are given for guidance.

Reason for Implementation

7. Key Benefits are shown in the table below:

Improved Accessibility	The addition of metadata will make it easier for staff both in the Department and outside to discover the information that is needed.

Customising Information	MOD staff often want to customise their information requirements. Metadata will aid this process and support the concept of profiling and establishing communities of practice.
Search Engine Configuration	Search engines can be configured to relevance rank results by the assigned metadata including subjects and keywords.
Improved Management of Intranet/Internet	Metadata will support the requirement for better management of the intranet and MOD internet sites for their ownership responsibility, currency and accuracy.
Quick Reference	Metadata provides a summary of the information held in a resource, and may provide a quick and convenient way for a user to gain some understanding of the content of a resource, without having to access the resource itself.
Improved Information Governance	Metadata supports information governance. It will establish the quality and context of the information, who owns or is responsible for the information, and security and access restrictions as well as legal obligations.

Applicability

8. The responsibility resides with the developers and MOD owners of the information systems, namely EDRMS, CMS and DMS.

Compliance Criteria

9. Information Managers must provide evidence that the EDRMS, CMS and or DMS is configured to comply with the MMS. This will include the mapping table between the system generated metadata and the MMS metadata. Furthermore MOD users can fulfil the minimum metadata requirement for information resources to be labelled correctly within the information system, in accordance with JSP 717 Using the MOD Metadata Standard.

10. CIS Projects are required to provide evidence that the Metadata Policy is referenced within the User Requirement Document (URD) by Initial Gate. CIS Projects are also required to provide evidence that the solution complies with the Metadata Policy within the System Requirement Document (SRD).

Supporting External Documents/Relevant Links:

- JSP 717 Using the MOD Metadata Standard
- MOD Metadata Standard
- e-Government Metadata Standard v3.1 – including:
  - Modernising Government: CM4310 Cabinet Office 1999, The Stationery Office.
  - Transformational Government Enabled By Technology: CM6683 Cabinet Office 2005, The Stationery Office.
- IX Principles

Contacts for this Policy

For guidance on applicability and implementation of this policy please contact DBS KI-ICAD Metadata 1 Tel: 01793 555083 or Mil 96381 5083. For more general policy enquiries please contact the CIO Information Coherence Policy team Tel: 01793 555433 or Mil 96381 5433.

MINISTRY OF DEFENCE

JSP 329 Chapter 5
MOD Enterprise Identifier Policy

Introduction

1. Identifier Management requires anything which needs to be individually referenced or catalogued electronically to be uniquely identified using a commonly implemented scheme. This allows synchronisation tools to match common entities from different data sources and build data structures containing information derived from different sources without the need to manage that information more than once.

Background

2. The delivery of a Global Information Infrastructure (GII) that will bring the C4I capabilities needed for the NEC environment requires the capability to uniquely identify entities within and across GII systems.

Policy

3. To produce a suitable identifier system, the following requirements must be met:

    a. Uniqueness - all entities of a particular type MUST be uniquely identified. The system must not allow re-use of an identifier even when the entity is no longer relevant to the MOD, because the same entity may become relevant again later (ie a person leaving the Forces and later gaining employment as a Defence Contractor, Consultant or MOD Civil Servant must retain their original ID).

    b. Scalability - the identifier system MUST scale to meet any foreseeable requirement. Thus entity types having many entries (such as Person, Smart card, Role, Aircraft etc) must be able to uniquely identify each entity. Furthermore the system must be able to cope with the maximum foreseeable number of entries (realistically numbered in millions rather than thousands to meet future needs). The system must also be able to extend the number of different entity types supported with almost no practical limits.

    c. Usability - the identifier system MUST be straightforward to implement from a technical and policy perspective. It should also be simple to use and applications using it must be able to locate required entries quickly and easily.

    d. Interoperability - the identifier system MUST be capable of supporting information exchange with MOD coalition partners, such as NATO and CCEB nations, and collaboration with industry partners. As a minimum the identifier system must support multi-national defence networks, such as UK MOD – United States Department of Defense (US DoD).

    e. Object Type - in order to identify the type of object (unit, device, location, person etc.) to which the identifier relates it will be necessary to use a globally unique prefix "seed" identifier capable of interpretation by all NATO members. The Object Identifier described in JSP 457 is the system mandated for issue and control of object type identifiers.

f. Backwards Compatibility and Future Proofing - reverse engineering existing systems can be costly therefore the identifier system must not only meet the needs of current MOD projects but should also be capable of quickly and easily interfacing with existing identifiers and known future projects.

Reason for Implementation

4. The ability to accurately identify the same entity such as an individual or asset, across different GII systems, will be a critical component in achieving information superiority in the Battlespace.

Applicability

5. Any new projects or systems that will be employing an identity management system or systems to uniquely identify entities for which they have a responsibility. There is currently no intention to mandate changes to legacy systems to comply with this Policy.

Compliance Criteria

6. Projects must provide evidence that the MOD Enterprise Identifier Policy is referenced in their User Requirement Document (URD), as either constraints or requirements, at Initial Gate.

7. Projects are required to provide evidence within their System Requirements Document (SRD) that the solution complies with the MOD Enterprise Identifier Policy by Main Gate.

Supporting External Documents/Relevant Links

8. Volume 2 of JSP 457

9. Person Unique Identifier (PUID) is an example that meets all the Enterprise Identifier Requirements. Specific policy relating to the PUID can be accessed in Annex A.

Contacts for this Policy

10. Please contact the CIO Information Coherence Policy team Tel: 01793 555433 or Mil 96381 5433.

MINISTRY OF DEFENCE

JSP 329 Chapter 5 Annex A
Person Unique Identifier (PUID) Policy

Introduction

1. The PUID is an instance of a general unique Object Identifier and can be used to identify every individual within a community. For the MOD, it provides a unique, universal key which IT systems can use to identify persons and all data related to them.

Background

2. The need for a PUID arises from the historic plethora of schemes used to identify Service and Civilian personnel within the MOD. Current identification schemes range from security Unique Reference Numbers to individual Service and Staff Numbers. As a result, information on personnel is fragmented and very often duplicated across a number of databases designed for different purposes. Whilst extremely inefficient in terms of data capture and storage, this also results in gaps in corporate knowledge. Interoperability and the provision of coherent authoritative reference information to Defence are only realisable with unique identifiers. The PUID scheme provides a common identification system whilst retaining mapping to the legacy numbering systems.

PUID Policy

3. A PUID is defined as an Identifier that uniquely identifies a Person within or of interest to the UK Defence Community. To provide maximum utility, the PUID must meet the following top-level requirements:

    a. All personnel working within the MOD MUST be allocated a PUID which shall be unique throughout the MOD.

    b. The PUID SHALL cater for personnel both employed within the MOD as well as those who originate outside the community (such as NATO Service personnel, contractors etc) who may be regarded as information objects in MOD systems.

    c. It SHALL remain constant throughout and beyond an individual's career within the MOD.

    d. It SHALL not be reused.

    e. It SHALL support mapping to legacy system identifiers.

    f. It SHALL be based on a 32 bit digital word size and the numbering will start at 1,000,000,000 such that the printed representation is always the same length (10

characters).

g. It SHALL have a memorable 'user friendly' representation, known as the PUID Name, which shall be useable for electronic addressing using current international exchange standards.

h. The PUID Name SHALL a string of no more than 20 characters based on surname and initials plus 3 numbers. (The PUID Name may change for reasons of marriage etc, but the PUID will remain constant.)

i. All new applications being designed for the MOD that utilise data linked to personnel MUST incorporate the ability to utilise the PUID scheme.

j. Technical policy for the construction and use of PUIDs can be found in Volume 2 of JSP 457.

Reason for Implementation

4. Consistent naming, addressing and numbering of objects within UK Defence are crucial for the successful federation and interoperability of disparate systems. This can only be achieved if all Sectors and Agencies work to common guidelines and procedures through a central registration authority. The Director Information Systems Services (D ISS) is the top level registration authority for UK Defence. Within D ISS, the C4 Technical Architect team (C4TA) is responsible for Object Identifier (OID) and Directory Naming Policy, via JSP 457, whilst the Defence Information Infrastructure Project Team (DII PT) provides the central registration authority for PUIDs.[1]

5. Initial allocation of PUIDs within the MOD has been in the context of IT account management. In line with the above policy, PUIDs are therefore currently issued under the control of the DII PT against the contract held by Atlas (DII Future). However, DII PT, or any contractors working on their behalf, must comply with the detailed technical policy contained in JSP 457. The OID for PUID is: 1.2.826.0.1310.1.4.5

Supporting External Documents/Relevant Links:

- IX Principles
- Volume 2 of JSP 457

Contacts for this Policy

Please contact the CIO Information Coherence Policy team Tel: 01793 555393 or Mil 96381 5393.

[1] DINSA (Defence Interoperable Network Services Authority) has now been absorbed by C4TA

MINISTRY OF DEFENCE

JSP 329 Chapter 6
Electronic Unit Name (EUN), Appointment and Electronic Role Name (ERN) Policy

Introduction

1. This Policy defines how EUNs and ERNs are to be established for DII(F), Chots, DENNIS and other platforms. It replaces all previous high level policy documents on this subject, but contains no significant change in policy. If required for contractual purposes, the original superseded policy can be found at: DGInfo/6-7-6-Role Naming dated 17 Aug 06.

2. EUN is defined as the abbreviated name for a unit that is determined by a Top Level Budget (TLB) or Defence Agency and provides a unique reference for electronic messaging and identification purposes. The first aim of the Policy is therefore to enable email addresses or ERNs to be easily found by users, who may be unfamiliar with the unit, and to facilitate interoperability with other systems, in particular Bowman. However, as a unique identifier for unit, the EUN provides the potential to exploit information linked or related to a unit, and may be utilised by any number of applications for this purpose (it already features on situational awareness maps and is used for planning operational deployments). This Policy therefore also aims to maintain the utility and helps to ensure the quality of EUN as a unique identifier.

3. In this document:

    a. Unit refers to a unit as determined by the owning TLB organisation, for inclusion in its electronic form, in the MOD EUN List.

    b. Appointment refers to a post within a unit (also to accounts set up to support multiple users, such as watchkeepers).

    c. ERN refers to the entire name (i.e. Unit and Appointment). The general format for an ERN is:

< EUN >-< Appointment >

Electronic Unit Name

4. TLBs are responsible for determining EUNs. Generally,[1] EUNs MUST only be created to identify units that meet the criteria below and are **NOT** to be created for any other purpose. When choosing EUNs, TLBs must aim for brevity, clarity and consistency. If the name is too long, it will be cumbersome and reduce the number of characters available to represent the Appointment; if too short, it will lack meaning and be difficult to understand for those not familiar with the abbreviation, The rules and guidance for establishing EUNs are as follows:

[1] There are just two exceptions that may be allowed these are:

To identify special group mailboxes dealing with a particular subject. The EUN “Low flying” is one example of this and has been set up as a group mailbox for all low flying complaints.

Where an EUN is necessary for a temporary period to facilitate system trials.

a. In general, an EUN SHOULD be allocated at the level which corresponds to common understanding of what comprises a unit within that TLB: for example for Navy Command a ship, for Land a regiment or battalion, for Air a station or squadron.

b. TLB and Front Line Command Headquarters (HQs) contain multiple organisations at high levels of command. Sub divisions within these organisations will normally each require their own EUN down to and including 1* level.

c. In independent HQs, Unit Names SHOULD normally be the name of that HQ. However, no EUN can start with the prefix of 'HQ'.

d. In MOD departments, the Unit Name SHOULD normally be that in common parlance.

e. A unit is only allowed one active EUN at any one time. Therefore, when a new/replacement EUN is requested, the existing EUN MUST be deleted from the active column in the EUN database but displayed in the legacy column against the new EUN. This will allow previous role names to be used during a limited transitional period, but prevent new ERNs being created using the legacy EUN.

f. When requesting a new EUN, TLBs are REQUIRED to identify the parent of the unit for which the EUN is requested. This is to enable organisational information to be constructed from the EUN list. The parent in this context is the unit which exercises immediate command authority. So for a regiment, the parent is likely to be a brigade and for a brigade a division etc. This principle applies regardless of whether or not the unit is hosted by a larger formation for administrative purposes.

g. In general, Unit Names themselves SHOULD NOT be used to define hierarchy in command structure. However, there are circumstances where this may help to differentiate between similarly named units, so is allowed.

h. EUN is independent of location. Many units will have sub units located or hosted at different locations and even in different countries. However, this is not a reason to request EUNs for sub units.

i. Consistency within TLBs is important. The same style of abbreviation SHOULD be used for all similar units.

j. Bowman has specific data exchange restrictions. Therefore, where a Bowman Unit EUN exists, the identical name MUST be used. The rules for the compilation of Bowman EUNs are more restrictive than those required for DII.

k. Where abbreviations are already in common parlance, then these SHOULD be used.

l. Where abbreviations are not currently used they SHOULD only be created when the gain from brevity will exceed any loss of clarity.

m. An EUN can have a minimum one and maximum three parts, separated by spaces. The basic syntax rule is that EUNs MUST be alphanumeric, maximum 16 characters including spaces, but full details on syntax will be found in JSP457 Volume 3

Appointment and Role Names

5. The Appointment must also optimise brevity and clarity. Names must follow common standards, both in the order, and through use of common abbreviations. The rules and guidance for establishing the Appointment Names are as follows:

a. The Appointment Title SHOULD reflect the organisational hierarchy within the unit (higher levels first), so that all appointments within a particular functional division are grouped together. Title changes may well incur costs so care must be taken to avoid unnecessary change and, provided applied consistently, not every management level need be reflected.

b. Hyphens can be used to separate different fields within the Appointment (up to a maximum of 4 fields). Indeed, the first hyphen indicates where the EUN ends and the Appointment begins (see paragraph 3 above). However, with the exception of ERNs that utilise Bowman systems, spaces are generally preferred; this is to aid readability within the Global Address List (GAL) and directories.

c. Standard abbreviations for Appointments common to many units MUST be used whenever applicable. Abbreviations specific to a particular unit may only be used if no common abbreviation is available. The approved list of abbreviations for the creation of ERNs is at Annex A. This has now superseded the similar list at JSP457 Volume 3 Annex A, which is no longer authoritative and is not to be used for this purpose.

d. Use of specific rank, grade or title within Appointment Name is discouraged. However, if used MUST appear at the end of Organisational Appointment detail.

e. Appointments directly supporting senior officers SHOULD be given ERNs that will cause them to be sorted together with the Senior Officer Appointment.

f. A role occupant's name MUST NOT appear in the ERN.

g. Space and Round Bracket characters are stripped from the messaging address, so are not significant for uniqueness. Units and TLBs MUST ensure that, after the removal of these non significant characters, no duplications can occur.

h. To enable automatic translation between the respective messaging systems, where there is a one-for-one match between a DII(F) appointment and a Bowman address, then the DII(F) appointment MUST be identical to the Bowman address.

i. Appointments created for multi-access roles (e.g. watchkeepers) will follow the same general rules as standard appointments. The appointment SHOULD be clear that it is for a multi access role.

j. The two basic syntax rules are that:

   i. Appointments MUST be alphanumeric, with hyphens or spaces as separators.

   ii. The maximum ERN length (including hyphens and spaces) is 32 characters.

Further detail on allowable syntax can be found in JSP457 Volume 3

Responsibilities for EUN Registration

6. Besides the applicant, there are at least three other offices involved in the EUN registration process. These are the TLB Information Manager (IMgr), the Chief Information Officer (CIO) Information Coherence Policy team (who enforce policy on behalf of the Chief Information Officer), Defence Business Systems (DBS) KI-ICAD who check, enforce and approve EUN submissions against CIO policy, and the Contractor who maintains the EUN database. All applications that relate to a unit which could be equipped with Bowman will also need to be approved by the Land Environment Reference Information Capability (LERIC) acting on behalf

of the Signal Officer in Chief Army (SOinC(A)).

7. An EUN Application Form with a flowchart of the EUN registration process, instructions for completion and contact details for each of the TLB IMgrs can be downloaded from the Defence Intranet. The site also provides access to the EUN List Responsibilities for completion of the process are as follows:

    a. The applicant will complete the EUN Request Form and forward to the relevant TLB IMgr for initial approval.

        i. If it is not a Bowman unit (nor expected to become one), and the TLB has ensured that the application satisfies its own policy and criteria for EUNs, the TLB IMgr will forward to ICAD for final approval.

        ii. If it is a unit that has the potential to be equipped with Bowman, then the TLB IMgr will forward to LERIC who will check the consistency and validity of the name and that it conforms to the character restriction of Bowman systems. If compliant, LERIC will then forward to DBS KI-ICAD for final approval.

    b. DBS KI-ICAD will ensure that there are no conflicts with the EUN policy and, if necessary, discuss issues of omission, brevity, clarity and consistency with the TLB IMgr. When DBS KI-ICAD is content, the form will be forwarded to the Contractor responsible for maintenance of the EUN database.

    c. The Contractor will enter the new EUN and update the database with the information contained in the application form. Following this action, the Contractor will notify the unit that the registration process has been completed. The Contractor will also submit regular updates of the database for uploading and viewing on the Defence Intranet.

Supporting External Documents/Relevant Links:

- IX Principles
- JSP457

Contacts for this Policy

Please contact the CIO Information Coherence Policy team Tel: 01793 555391 or 96381 5391.

MINISTRY OF DEFENCE

JSP 329 Chapter 6 Annex A
A List of Approved Abbreviations used in Electronic Role Name Construction

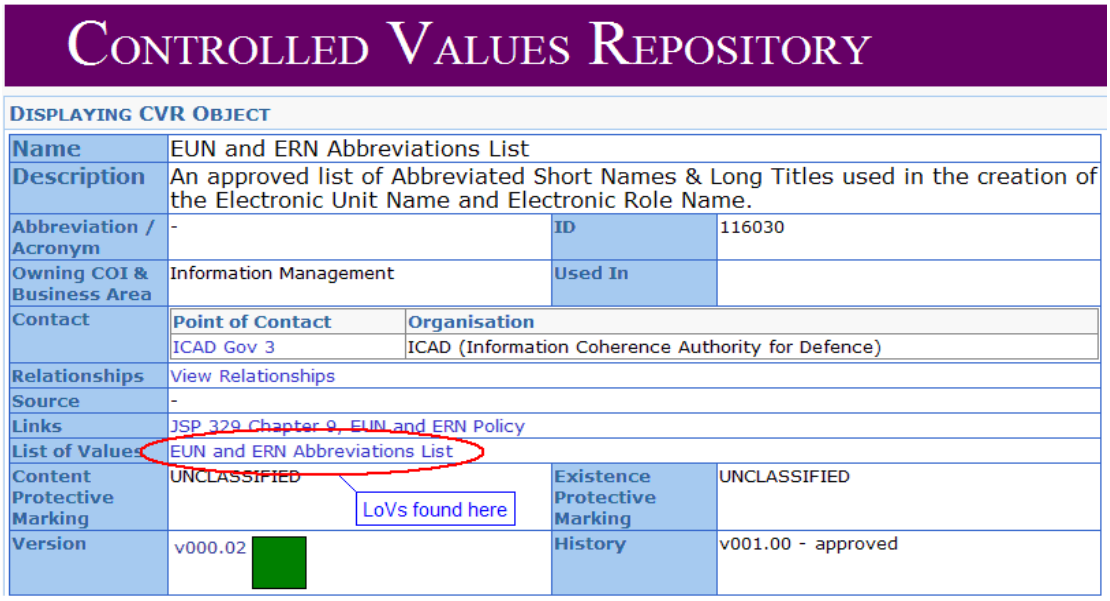
1. The list of Short and Long Name terms found in the Controlled Values Repository (CVR) has been produced with the sole aim of improving coherence within Electronic Role Names (ERNs) to make them more widely understandable and intuitive. When constructing ERNs, information managers are mandated to use these abbreviations. The list is authoritative for this purpose alone but is not exhaustive. Any suggestions for amendments or additions to the list should be forwarded through the instigator's respective TLB for consideration. See TLB contact information below.

2. The use of capitals in the post title is not obligatory unless normal service usage dictates otherwise; a mixture of upper and lower case is acceptable, especially where it promotes clarity. However, use of different case does not confer uniqueness.

3. Where more than one short name is to be combined each element's initial letter SHOULD be capitalised within the compound, and spaces omitted, ie 'CamelCase'. Thus Assault Pioneer Warrant Officer can be seen as comprising three recognised abbreviations 'Asslt+Pnr+WO' which, when combined, will become 'AssltPnrWO'. There will be some exceptions to this, such as military ranks where spaces may be used for example Lt Col but, as with different case, the space does not confer uniqueness.

4. The ampersand can cause problems with electronic records storage systems. Ampersands are therefore not to be used as part of an ERN.

5. A link to the approved list of abbreviated short names and long titles can be found in the CVR under the title of 'EUN and ERN' Abbreviations List. The CVR object diagram below indicates the URL link to the 'list of values' LoVs used for EUN and ERN creation.



6. For further guidance on EUN/ERN formulation please refer to the list of Authorised Information Managers (IMgrs) or TLBs listed within the EUN application form for assistance.

MINISTRY OF DEFENCE

JSP 329 Chapter 7
Defence Unit Identity Number - Policy and Management

Introduction

1. This Policy defines how Unit Identity Numbers (UINs) are to be created, controlled and managed; it replaces all previous policy documents and instructions. The aim of this revised policy is to provide clearer direction and governance so as to bring greater coherence to the application and approvals processes for all UINs.

Background

2. The UIN was introduced in 1971 to enable Defence IT systems to use a common 'data item' to identify units, sub-units, organisations or groupings of organisations within the MOD. (NB: *Throughout the remainder of this document, the term 'unit' is used to describe the entity linked to a UIN.*) Over the years, the uses to which UINs are put have grown to cover a wide range of tasks for which they were neither originally designed nor intended. These tasks can now be broadly categorised as:

a. Asset Management
b. Liability Management
c. Financial Management
d. Liability Planning
e. Location Information

However, as requirements expanded, non-standard ways of working have developed such that different types of UIN evolved. In this Policy, these are referred to as standard and non standard UINs. Further information on both types of UIN is provided below.

3. This Policy now enforces a single gate application route for all types of UIN. To achieve this, it has been necessary to redesign the UIN application form (MOD F942 accessible here) which now includes additional guidance on the correct routing for each application. All previous versions of this form have therefore been superseded and are no longer to be used.

Governance

4. The Chief Information Officer (CIO) is the Authority for UINs and has responsibility for formulating policy. Responsibility for the day-to-day husbandry of all standard UINs is delegated to Army Information Services (AIS) Branch, CBM Division, HQ Land Forces. Responsibility for final authorisation of all non standard UINs (CA, CB etc) is delegated to Defence Equipment and Supply Chain Management (DE&S SCM). Responsibility for the day-to day husbandry of non standard UINs is delegated to Defence Equipment and Support, Joint Support Chain Services (DE&S JSC Services).

Policy

5. There are two main functions that both types of UIN perform; these are to identify the unit and to link the unit to a location. It therefore follows that any change to either the unit, the unit name or location (including postcode) must be reported and acted upon at the earliest opportunity.

6. Applications for the creation, amendment or end-dating of **all types** of UIN must follow the approval route described in the following guidance and application form MOD F942[2]. When authorising UIN changes, TLB Authorisers will need to follow individual TLB procedures to ensure that all appropriate parties are informed when changes occur so that systems such as JPA, which use UIN data, remain aligned. However, these procedures will vary considerably between TLBs and are therefore outside the scope of this policy.

7. No application will be acted upon without the prior endorsement of the appropriate TLB.

8. With the exception of Custodial Accounts (CA UINs) where units are holding stock to be issued to others, no unit or sub-unit is to be allocated more than one UIN.

Standard UIN

9. Creation. Full guidance on the UIN creation process is embedded within the application form. However, prior to raising a new request, potential applicants are to check that a UIN does not already exist. The next 2 paragraphs explain how this may be done.

10. SLA and UIN Interim Management System (SIMS). SIMS manages, collates and provides authoritative UIN information for authorised users and information systems across Defence. It is connected to DII and, for read only purposes, a link to it can be found on the System for Liability Information Management (SLIM) team site here. Alternatively, search for 'SLIM' on the intranet and follow the link.

11. Search. Information on all standard UINs can be accessed via a UIN Search web page which is listed under Related Applications & Tools on the SLIM team site. Currently this information encompasses Long and Short UIN Name, Address, Post Code and Budget Hierarchy.

12. Format. A standard UIN consists of 3 elements comprising 6 characters, the first and last being alphabetic with 4 numeric characters between as shown below:

A1234A

The first character represents the Front Line Command (FLC) or Department to which the UIN belongs while the last character is used to indicate if the UIN represents a unit or a sub-unit thereof. The letter A when appearing as the last character always indicates that the UIN represents a unit while any other letter indicates a sub-unit. There is no order of precedence conveyed by the letter that appears and no limit, other than the available characters, to the number of sub-units that may be represented.

13. FLC and Department Characters. The authorised list of characters associated with FLCs and Departments is shown in the table below:

Character	FLC/Department
A	MOD (A) / Army
B	Infrastructure Accounting Army
D	MOD Central / Joint Service
F	MOD (RAF) / RAF
J	Non Budgetary UIN
N	MOD (Navy) / Navy
P	Defence Equipment & Support
T	Army / Combined Cadet Force

[2] Applicants should note that local or specific TLB instructions may also apply. However, where any contradiction arises, this Policy will take precedence.

However, it should be noted that although Special Forces units and any UINs associated with them must be authorised by Central TLB, the first character in their UINs will reflect their main Front Line Command.

14. Unit Identifier. The main body of the UIN consists of 4 numeric characters which, together with the preceding and following alphabetic characters, will be unique within each FLC or Department.

15. End Dating. Standard UINs are never completely deleted since they may be required for audit or historical purposes. However, when they are no longer required by the unit (such as when the unit closes or disbands) a MOD F942 is to be submitted to record this fact. This will result in the UIN being given an End Date after which it may no longer be used for financial or supply transactions. However, it should be noted that a UIN cannot be End Dated if there are sub-units that remain extant. Advising of UIN End Dating is a unit responsibility. However, in cases where the unit has already disbanded, responsibility will default to the appropriate TLB Budget Manager (TLB BM).

Non Standard UINs

16. Custodial Account Unit Identification Number (CA UINs). UINs with the prefix "CA" are associated with the Army's Base Inventory System (BIS), often referred to as Stores System 3 (SS3). The CA UINs are used by Army stockholding units and contractors to account for Defence materiel and enable demands to be placed for materiel supplied through this system. Other Non Standard UINs generally only allow material to be supplied against special authorisation. The prefixes of all Non Standard UINs, together with the uses to which they are put, as well as the main users of each prefix are shown in the table below:

Prefix	Use	Users
CA	To manage stock on behalf of the Joint Support Chain (JCS).	Joint Support Chain Services (JSC Services) Royal Engineers (RE) and Royal Logistic Corps (RLC) contractors when authorised.
CB/CC[3]	To allow Delivery and Project Teams (DTs) & (PTs) to authorise contractors to receipt and consume stock in support of contracts.	DE&S DTs & PTs
CP	To manage the issue of materiel to contractors for contract repair.	DE&S
CQ	To enable issue of stock to contractors for disposal.	Defence Sales Agency (DSA)
CR	To manage repayment issues to other government departments and contractors.	JSC Services
CW	To manage the issue of operational stocks held as war reserve.	JSC Services
NP	To manage the issue of materiel to sea cadets/scouts and combined cadet forces.	Naval Command

Non standard UINs are entered on the Demand Referrals Errors and Address Management System (DREAMS) which is maintained by JSC Services.

17. The initial approval route for non standard UINs will be the same as that of standard UINs. Therefore, all requests for creation/amendment/End Dating of non standard UINs are to be made on F942. The guidance on the form will direct applicants to the correct authority for approving the application. However, non standard UINs will only be approved for the uses shown in the table above.

[3] When all available numbers have been issued, this series can be expanded to include the additional prefixes of "CD" "CE" etc.

18. Maintenance of the Non Standard UIN Database. JSCS Unit Locations is responsible for the allocation, amendment and End Dating of all CA UINs once the correct authorisation has been given.

Operational UINs

19. Land Forces Units are not to deploy on Operations with their own peacetime UIN unless instructed to do so by CSS Ops/Cts, HQ Land Forces. Operational UINs will be requested through SO2 Log Ops/PEPs, by submitting a F942 prior to the commencement of the operation or deployment. Should they be required, Sub Unit UINs can be created using the same procedure. Units deploying on operations that are not allocated a specific UIN, will use the existing Operational UIN. An Operational Unit Title will be allocated to all operational UINs and this name will generally remain for the duration of the Operation. On roulement Units will take over this title in Theatre.

Amendment to UIN Details

20. If a unit with a UIN changes its title, location or any other information previously provided, the details of those changes must be submitted on a new MOD F942 via the routing outlined on the form. This also applies to operational UINs. However changes to an operational unit title or listed address/location must be authorised by SO2 Log Ops/PEPs. Operational units are not to change titles without this authority.

Financial Aspects

21. A high proportion of standard UINs are also used to apportion financial costs between the correct budgets. These UINs are provided by SIMS (as the single source of standard UINs) and managed within the Departmental Chart of Accounts (COA), which defines the budgetary hierarchy. This is recorded on the Standing Data System (SDS) maintained by Director Financial Management (DFM) and regular feeds of COA/SDS data are provided to many systems for validation. It is therefore important that whenever any UIN (even non-standard) is created or amended proper consideration is given to a valid Budgetary Structure to enable accurate cost capture.

Supporting External Documents/Relevant Links

JSP 886 Vol 3 Pt 15
SLIM Team Site
F942

Contacts for this Policy

22. For questions directly related to policy, please contact CIO Information Coherence Policy team Tel: 01793 555393 or Mil 96381 5393. Questions related to the approval of applications should be referred to either the appropriate TLB budget manager or, depending upon the progress, AIS Branch, HQ LF, for standard UINs and JSC Services for non standard UINs. Contact details are contained in the application form (see F942 link above).

MINISTRY OF DEFENCE

JSP 329 Chapter 8
Information Coherence and Governance

Introduction

1. CIO, working together with the Defence Business Services (DBS) organisation, is responsible for developing information coherence policy and promoting an agreed controlled vocabulary that is usable throughout Defence; thereby improving interoperability between present and future information systems to support enterprise planning. Interoperability will be improved, with future systems being designed and built to recognised information exchange standards to which legacy systems can also be mapped. Central coordination will provide Defence with a means of adopting information exchange standards that future systems can be built to and legacy systems can map to. However, governance is required to ensure these standards are adopted.

Background

2. Projects are driven by time cost performance envelopes and this process, by its nature, encourages conflicts in priorities that projects must make in order to come in on time and budget. This often results in a stove-piped approach that does not properly take into account wider Defence requirements, contributing to a lack of coherence in the information held in MOD systems. As a result, different people looking for the same facts do not get consistent answers and the way the MOD currently stores and retrieves information is inefficient and does not make it easy to find what is needed. Non standard interfaces are developed resulting in significant resource and effort each time a requirement to exchange data is identified.

CIO Approach

3. Information must be managed properly as required by the business, good practice, the legislation applicable to public records and the Freedom of Information Act. MOD is therefore required to ensure that users are consistent in their approach to information management and use of standards. A balance is required between freedom of action and discipline; adherence to basic rules relating to information storage and retrieval is paramount and common agreed standards must be put in place to enable effective information exchange and reduce duplication.

4. The governance authority that CIO wields will flow from the Defence Management Board, through the Chief Information Officer Forum, the MOD Information Strategy (MODIS) Executive Group and the Enterprise Architecture Working Group to the Data Management Strategy Technical Implementation Working Group led by DBS KI-ICAD AstHd. This will ensure that the strategic direction and policy development is in accordance with wider MOD policy. There are a number of ways in which CIO intends to achieve an effective governance regime and these are identified below:

a. JSP 600 leaflets will support and draw the attention of project managers to the policies contained in JSP 329.

b. Policy compliance will primarily be driven by the Network Technical Authority (NTA) through its Integration Assurance (IA) teams and scrutiny processes. However, this will also be augmented by subject matter expertise provided by CIO which will have the authority to inspect the evidence supporting compliance when it is deemed necessary or appropriate. CIO will liaise closely with the IA teams and may also undertake some scrutiny, on a sample basis, of CIS projects that would otherwise fall below the thresholds of the IA teams.

c. CIO will provide the focal point for information coherence between Defence, Government, NATO and international bodies.

d. CIO will adopt a Communities of Interest (COI) approach to information management. DBS, through DBS KI-ICAD, will ensure that COIs are established and stakeholders identified for each specialist area within Defence.

e. COIs will be established along the Defence Lines of Development (DLODs). (See related documents/links below.).

f. Working Groups will be identified or established for each COI. Each group will be responsible for the following functions:

I. Communications strategy across the COI.
II. Definition and terminology issues management.
III. Benefits/Risks management.
IV. Coherence of instructions and guidance on information coherence policy within their community.
V. Proposing changes to JSP 329.

Further information on COIs is at Annex A and a representative view of COIs and the governance chain can be found at Annex B.

Supporting External Documents/Relevant Links

- Controlled Values Repository (CVR)
- 2005DIN03-12 Defence Lines of Development
- CVR User Guide
- CVR Processes, Objects and Roles
- MOD Information Strategy (MODIS)
- Data Management Strategy (DMS)

Contacts for this Policy

Please contact the CIO Information Coherence Policy team Tel: 01793 555433 or Mil 96381 5433.

`

MINISTRY OF DEFENCE

JSP 329 Chapter 8 Annex A
Communities of Interest (COIs)

1. A COI is a group of stakeholders with a shared interest in a specific subject area or business output. They will be nominated to represent the business needs of their organisation within the MOD. Members of a COI will have a common goal of improving information sharing as well as the establishment of agreed information standards.

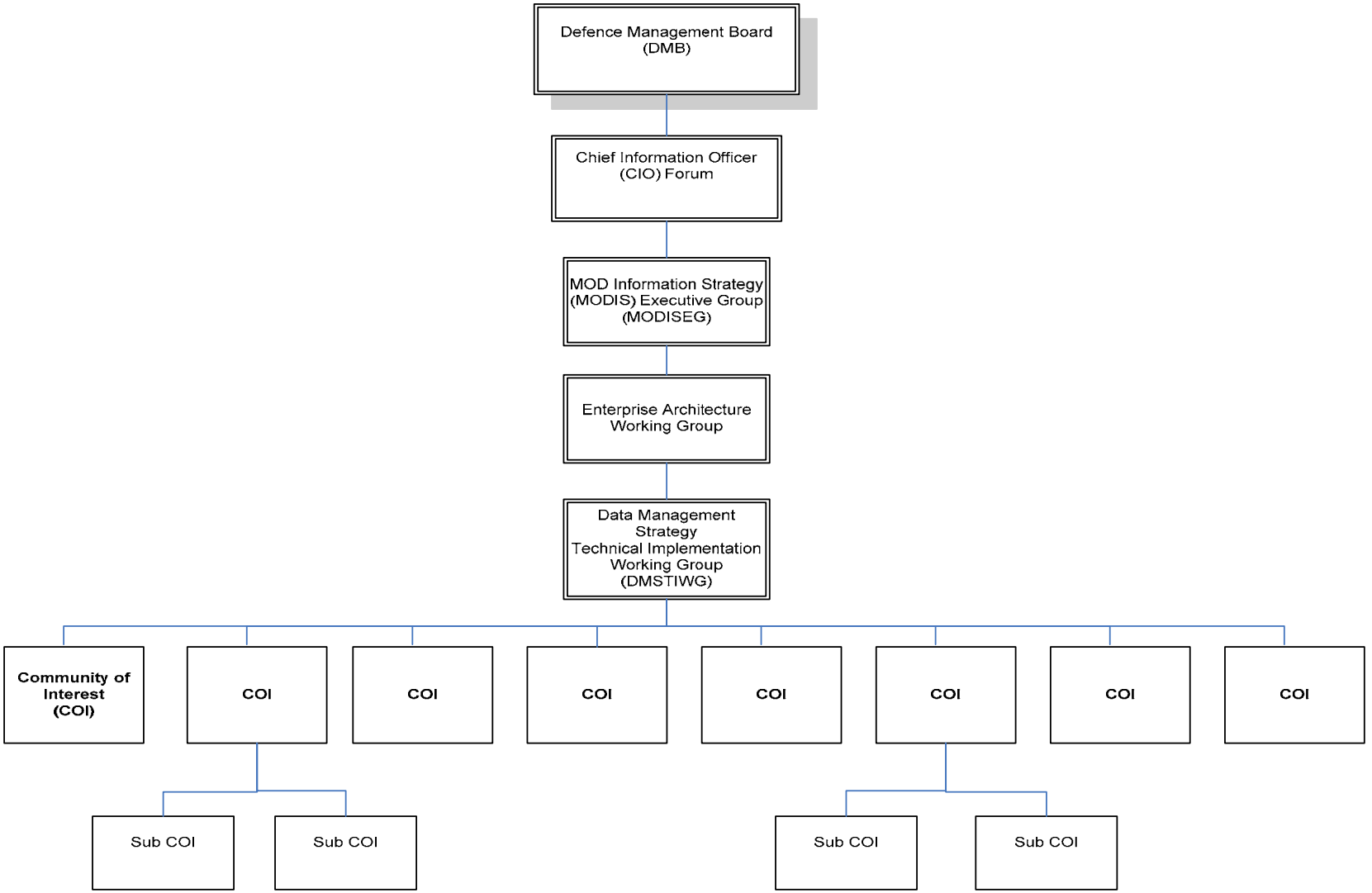
2. COIs are key to managing the complexities of information interoperability and access to data. They will add value by establishing agreed standards and by taking ownership of key elements of corporate data. Bringing expertise in their own fields, they will improve data management and sharing across Defence.

3. A COI is likely to operate most effectively if its members are drawn from across MOD organisations (thus encompassing a broad range of expertise) rather than from the same branch or directorate. Widespread membership is therefore encouraged and there is no restriction on the number of COIs to which an individual can belong.

4. Data and information managed in, or referenced through, the CVR will support a COI approach along the Defence Lines of Development.

5. For more information, Please contact the CIO Information Coherence Policy team Tel: 01793 555433 or Mil 96381 5433.

JSP 329 ANNEX B TO CHAPTER 8
CIO GOVERNANCE
OVERVIEW



MINISTRY OF DEFENCE

JSP 329 Chapter 9 Glossary and Abbreviations

ADS	Authoritative Data Source
ARD	Authoritative Reference Data
BSI	British Standards Institution
C4TA	C4 Technical Architect team (DINSA is now a function of C4TA)
CCEB	Combined Communication & Electronics Board
CIO	Chief Information Officer
CIS	Communication Information Systems
CMS	Content Management System
COI	Community of Interest
COIs	Communities of Interest
COTS	Commercial off the Shelf
CVR	Controlled Values Repository
DBS	Defence Business Services
DEAP	Defence Enterprise Architecture Portal
DEC CII	Director Equipment Capability Command & Control Information Infrastructure
DG INFO	Director General Information
DIN	Defence Instruction Notice
D ISS	Director Information Systems Services
DGIWG	Digital Geospatial Information Working Group
DII PT	Defence Information Infrastructure Project Team
DLODs	Defence Lines of Development

DMS	Data Management Strategy
DPO	Defence Process Owners
ebXML	e-Business eXtensible Markup Language
EDRMS	Electronic Document & Record Management System
e – GIF	Electronic Government Interoperability Framework
e – GMS	Electronic Government Metadata Standard
ERN	Electronic Role Name
EUNs	Electronic Unit Names
GAL	Global Address List
GII	Global Information Infrastructure
GML	Geographic Markup Language
IA	Integration Assurance
ICAD	Information Coherence Authority for Defence
IMgr	Information Manager
ISO	International Standardisation Organisation
IWG	Information Working Group
IX	Information Exploitation
JSP	Joint Service Publication
LERIC	Land Environment Reference Information Capability
LoV	List of Values
MMS	MOD Metadata Standard
MODAF	MOD Architectural Framework
MOUMG	Memorandum of Understanding Management Group
MODIS	MOD Information Strategy
NATO	North Atlantic Treaty Organization

NEC	Network Enabled Capability
NTA	Network Technical Authority
OGC	Open Geospatial Consortium
OGD	Other Government Department
OID	Object Identifier
PPPA	People, Pay and Pensions Agency
PT	Project Team
PUID	Person Unique Identifier
RFC	Request for Comments
SPVA	Service Personnel & Veterans Agency
SRD	Systems Requirements Document
STANAGs	Standardisation Agreements
TLB	Top Level Budget
UIN	Unit Identity Number
UBL	Universal Business Language
UKDT	UK Defence Terminology
URD	User Requirements Document
US DoD	US Department of Defense
W3C	World Wide Web Consortium
WSDL	Web Service Description Language
XML	Extensible Markup Language
XSD	XML Schema Definition
XSLT	Extensible Stylesheet Language Transformations

MINISTRY OF DEFENCE

JSP 329
Frequently Asked Questions and Scenarios

Q: Why can't I create and hold my own list of data values? It's much quicker and easier to produce my own.

A: If you are certain that the data you are producing can only be of use in your area then this may be acceptable. However, if the data might be used elsewhere, ie is of corporate value, it falls into the category of authoritative reference data. There can then be a significant overhead on maintaining that data and ensuring it remains fit for purpose. The data maintenance element through life is often overlooked during early planning stages and ends up causing issues later on in the project's life – especially if the system is likely to be used to produce data for management information purposes. If several projects are holding similar sets of data then they are all duplicating expense and resource to maintain it. A lot of MOD resource and effort goes into identifying and removing duplicate databases and addressing the problems caused by them. At a corporate level it is more efficient to put effort into the data requirements at the start of a project rather than have to address them later.

Q: Adding metadata each time I create and save a document is a waste of time. We use a sound file structure that everyone keeps to so I know where the documents are filed and can easily find them.

A: Metadata is data that describes the data being stored – this can be as simple as the date and time stamp on a photograph but its usefulness cannot be maximised unless it is consistently applied. Maybe you can find the documents now, but what happens when you move on? Moreover, the MOD has legal obligations requiring it to find relevant information – the Freedom of Information team for example may need to be able to find it and the only way they can do that efficiently is through the addition of consistent and accurate metadata which will allow it to search through all the records across the directorates. The Department will incur penalties if it fails to meet its legal obligations. Similarly if important information such as a key report required to support the front line cannot be found then the consequences may be more than financial. It may seem a lot of effort now because it is new and different but once people become familiar with the categories of information they use and have identified suitable keywords, defaults can be set up for each of the folders to automate the process and make it much quicker. DBS has subject matter experts available to help you do this if necessary.

Q: What is the difference between Reference Data (RD) and Authoritative Reference Data (ARD)?

A: RD is defined as persistent data and metadata that identifies, describes and constrains other data. ARD, on the other hand, is reference data that meets agreed quality criteria and is made available through the CVR. ARD is used to store, search, retrieve, share and inform, enabling the delivery of coherent information with confidence and accuracy. An example of RD is location data where it is currently stored across many platforms within Defence. An example of ARD would be where that location data was rationalised into a single repository, managed and maintained by a single Data Owner for Defence. Where data has been identified as being of benefit pan-Defence the MOD aims to eliminate as many alternative

sources as possible and focus on developing access to a master source that can be used with confidence. This conforms to the "store once use many" mantra by having a single authoritative source responsible for the provision and maintenance of that data across Defence.

Q: What is data management all about?

A: In a nutshell 'quality' – it refers to the processes put in place to help us achieve that. Good data management means that data will be defined and stored in a consistent manner so that it is accurate, relevant, up to date and more easily found and accessed. For example, if people put the same effort into making sure their eDirectory entry was accurate and up to date as they would if they changed their bank account details the accuracy of the MOD directory information would improve beyond recognition! Effective data management means that the MOD will have quality data to use in support of its operational and business activities. MOD's leaders often have to make difficult decisions – they have a better chance of getting it right if the information they have used to reach those decisions is absolutely correct and up to date.

Q: I'm running a project with tight timescales to meet – data and information management is nice to have but I haven't got time to waste on it.

A: How many times has equipment arrived at the wrong time and/or in the wrong place or else the wrong equipment to the right place at the right time? Unless MOD can get some coherence on its data, these types of scenarios will continue to be an issue.

Q: How do I apply to register a new Electronic Unit Name (EUN)?

A: The EUN application form can be downloaded from the Defence Intranet. Search against EUN and this should take you to a page with links to both the application form and the latest list of approved EUNs. The application form also contains guidance on the EUN registration process as well as contact details of the principal information managers who deal with EUN applications within each of the Front Line Commands and Top Level Budgets (TLBs).

Q: My Unit is located on many different sites across the country and some personnel are even based at overseas locations. Should we each register different EUNs?

A: No. EUN bears no relationship to location. Indeed it is very common for various elements which make up a Unit to be located in different places. It is also very common for Units to move location. Although there are exceptions such as RAF Stations, because of this, it is generally not recommended that the location forms any part of the EUN.

Q: What happens to my previous EUN when a new one is registered and will those still using the old EUN be disconnected from the e-mail system?

A: Each Unit will only be allowed to register one active EUN. However, it is recognised that transition to new systems will always take some time – particularly when a Unit is represented at many different locations. Because of this, unless specifically requested, wherever possible the previous EUN will be removed from the approved list but shown in the legacy column of the database against the new EUN. This will allow mapping to the old EUN which will continue to be used for messaging purposes until all people have migrated and have role names based on the new EUN. However, it should be noted that once a new EUN has been approved, no new role names may be created using the old EUN.

Q: Can I register an EUN for my section?

A: As a general rule no. The level at which an EUN is set is ultimately a matter for each TLB to determine. In general, an EUN should be allocated at the level which corresponds to

common understanding of what comprises a Unit within that TLB; for example, for Fleet a ship, for Land a regiment or battalion, for Air a station or squadron. Headquarters within Front Line Commands and Centre TLB contain multiple organisations up to 3* level. Sub divisions within these will normally each require their own EUN down to 1* or director level but, unless to meet a specific purpose, not usually below this.

Q: Why are old, redundant EUNs still displayed in the list of approved EUNs?

A: Experience has shown that whilst Units are usually ready to apply for a new EUN, removal/deletion of redundant EUNs has often been given a low priority. Also with policy lagging behind, governance was patchy when EUNs were initially introduced. This led to some anomalies.

The overarching EUN and Appointment and Role Naming policy is now contained in JSP 329 and a central governance regime has been introduced. With assistance from each of the TLBs, the quality of the data within the list has significantly improved. A main driver for the cleansing work was eDirectory which went live in December 2010 and uses the EUN data. Since eDirectory has now become the major source of MOD organisational data it is essential that the quality of that data continues to improve.