

JSP 602 Instruction	1008	Applicability	Applications, Data/Information, Integration
Configuration Identity	Version: 2.0 Reviewed: 2009-07-01	Epoch Applicability	2008 - 2010

## JSP 602: 1008 - Information Coherence Environment

### Outline

*Description:* The Information Coherence Authority for Defence (ICAD) is charged with bringing coherence to information across the MOD. Coherence will be achieved by improving the quality, availability and reliability of data, and standardising exchange mechanisms. This requires the production of commonly agreed definitions and vocabularies and setting the exchange standards that will underpin the MOD's corporate data architecture and provide information coherence across systems. This leaflet identifies the policies that support these principles: Data Definition, Corporate Reference Information (CRI), Electronic Data Exchange (including policy on the use of XML), UK Defence Terminology, Metadata and Enterprise Identifier (including Person Unique Identifier (PUID)). Full versions of these policies are contained in [JSP329](#).

*Reasons for implementation:* The achievement of Information Coherence will deliver benefits across the four pillars; Infrastructure, Information, People and Processes bringing commonality to the way the MOD defines and utilizes information. It will improve interoperability within Defence and see that the right information is available, in the right format, to the right people, at the right time. The policies contained within this leaflet define how the MOD will manage, exchange and view information by providing a framework for Information Coherence throughout Defence.

*Issues:* Failure to use consistent terminology will result in difficulties locating data and meeting legal requirements in areas such as Freedom of Information; it may also create data exchange issues. Multiple sources of the same data will increase maintenance costs and create confusion over accuracy and completeness. Non standardised formats will reduce interoperability and could lead to failure to meet internationally agreed standards. These issues are likely to impact on through life costs and potentially lead to operational errors.

*Guidance:* This leaflet falls within the scope of both the e-Government Interoperability Framework (e-GIF) and is consistent with NATO C3 Technical Architecture (NC3TA) and general management procedures for implementing the NC3TA in NATO C3 systems development.

### Overarching Policy:

Information Coherence will be improved through better data quality and making corporate information available to all who need it. Underpinning this will be agreed controlled vocabularies and exchange standards. Information must be treated and managed as one of MOD's most valuable corporate assets. Barriers to sharing and reuse must be identified and prevented or mitigated. There will be only one authoritative source for each element of Reference Information (RI) and each RI value will have a unique identifier; alternative sets of data are not to be created

or maintained. In other words, databases are not to be created or maintained to hold data that is already held elsewhere and unique identifiers will be used to identify and readily exploit the information we hold. (To prevent infrastructure and bandwidth overload, sub sets of master data may be downloaded for local use. However this must only be refreshed from the authoritative source.)

## Policy

### Strategic

#### **1008.01: Data Definition Policy**

**1008.01.01** The Data Definition Policy requires that data definitions used across the MOD must be approved and made accessible through the Controlled Values Repository (CVR). ICAD manages the CVR which is a web based service offering a single point of access to authoritative sources of RI. Agreed names will be unique within each Community of Interest (COI). Where available, information systems must adopt approved corporate data definitions to support information exchange. When systems interoperate it is essential that the meaning of the data to be exchanged is clearly understood. The integrity of information is ensured when the correct data is exchanged and systems are able to correctly interpret it. The mechanism for achieving this goal is to ensure that predefined, meaningful items of data are made available through the CVR. Information Systems which use an agreed MOD Interface Standard can exchange data between themselves using that standard. However, if these systems are required to exchange data with a system that uses a different Interface Standard then the corporate data definitions must be used. Off the shelf packages and legacy systems that are unable to use approved MOD data definitions internally are still required to exchange data with other systems using the corporate data definitions. Therefore additional interfaces may be required.

**1008.01.02** This policy applies to any project or system storing or exchanging data within the MOD or between the MOD and an external (non MOD) application. Legacy systems should also comply if financial constraints allow and implementation would be cost effective.

#### **1008.02: Corporate Reference Information Policy**

**1008.02.01** CRI Policy mandates that any person, project or system that will be storing or exchanging reference information throughout the MOD will only use approved CRI where it exists. Alternative sets of CRI are not to be created or maintained and any project considering the creation of reference data which may be of corporate interest must submit it to ICAD for scrutiny.

**1008.02.02** This policy applies to any MOD person, project or system that will be storing or exchanging reference information that is, or could be, of corporate interest.

*Comment:* Corporate Reference Information is defined as "Trusted non-business specific information provided by an authoritative source that can be readily exploited across Defence". It is authoritative reference information or controlled lists of values that is managed, maintained and used across more than one organisation, system or service. For example Person CRI (Person Titles, Nationalities, Ethnicity Tables etc) are managed and made available via the Service Personnel and Veterans Agency (SPVA) and People, Pay and Pensions Agency (PPPA). Only these sources are considered authoritative for MOD person data.

### **1008.03: Electronic Data Exchange Policy**

**1008.03.01** The Electronic Data Exchange Policy mandates that data to be exchanged, and exchange mechanisms, must be defined according to Open Standards. Where no appropriate Open Standard exists, data and exchange mechanisms must be defined in MOD compliant eXtensible Mark-up Language (XML). Data definitions used in information exchange, including XML definitions and schema, must be recorded in the CVR. The whole life cost of interfaces compliant with this policy must be part of the Investment Appraisal, Project Plan and the Through Life Management Plan. Plans for major upgrades or replacements of existing (legacy) applications must provide Open Standard or MOD compliant XML interfaces.

**1008.03.02** This policy applies to all staff responsible for UK Defence projects or for framing and/or implementing information strategies within MOD. It especially applies to staff and contractors responsible for the creation of applications within MOD.

*Comment:* XML is a method of tagging data that is widely accepted throughout industry and government. The tags used generally describe the meaning of the data and are defined by the user. 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.

### **1008.04: UK Defence Terminology Policy**

**1008.04.01** The UK Defence Terminology Policy mandates use of the UK Defence Taxonomy, that provides the subject category at folder level within a file structure, and the UK Defence Thesaurus which generates keywords to describe the document being stored.

**1008.04.02** This policy applies to MOD employees and contractors who store information on an Electronic Document and Record Management System (EDRMS), Document Management System (DMS) or a Content Management System (CMS).

*Comment:* ICAD provides the CVR which is a web based service offering a single point of access to the UK Defence Taxonomy and the UK Defence Thesaurus as well as authoritative sources of reference information.

### **1008.05: Metadata Policy**

**1008.05.01** The MOD Metadata Standard (MMS) is mandated for EDRMS, DMS and CMS, so every information asset created in these systems must be accompanied by metadata. Communication Information Systems (CIS) 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.

**1008.05.02** This policy applies to developers and MOD owners of the information systems, namely the EDRMS, DMS and CMS.

*Comment:* The CVR definition of metadata is “data about data”. It can be regarded as indexing, where additional information to describe and summarise the content of an information resource is stored and linked to it. For example metadata includes the creator/author of the resource, its title, the date it was created, the subject and security classification. The objective is for the automatic generation of as much mandatory metadata as possible. Also, to provide in the MMS the source for the controlled set of vocabulary values to be used for each metadata element. Adoption of the vocabulary defined within the MMS will lead to consistency in the description of data entities, and a corresponding improvement in the manner in which they are searched for and found.

**1008.06: Enterprise Identifier Policy**

**1008.06.01** The Enterprise Identifier Policy requires that all entities (see comment below) which need to be referenced electronically are uniquely identified using a common scheme. This allows synchronisation tools (such as MetaDirectories) to link data from different sources without the need to manage that information more than once. The technical requirements that must be met are contained in [JSP 329](#).

**1008.06.02** This policy applies to any new projects or systems that will be employing a system or systems to uniquely identify entities for which they have a responsibility. However, there is currently no intention to mandate changes to legacy systems to comply with this policy.

*Comment:* In relation to this policy an ‘entity’ can be described as a single person, place, or thing about which data can be stored.

**1008.07: Person Unique Identifier (PUID) Policy**

**1008.07.01** The PUID Policy mandates that all personnel working within Defence are to be allocated a PUID which shall be unique throughout the MOD. It shall remain constant throughout and beyond an individual’s career within the MOD.

**1008.07.02** All new applications being designed for the MOD that utilise personnel data must incorporate the ability to interoperate using the PUID.

*Comment:* PUID is a 32 bit binary number which is used as an identifier to uniquely identify a person within or of interest to the UK Defence Community. For IT account management purposes it is linked to a more user friendly PUID Name which is a combination of the person’s surname, 1<sup>st</sup> initial and a generated 3 figure number.

**Deployed**

As for Strategic domain.

**Tactical**

As for Strategic domain.

**Remote**

As for Strategic domain.

**Responsibility for Implementing the Policy**

Implementation of these policies shall be the responsibility of all MOD CIS projects and system owners. The policies apply to all information and knowledge stored within MOD as directed by the Information Management (IM) Handbook & Commanders Precis and JSP747 – Information Management Policy & Protocols. These Policies supersede JSP540.

## Procedure

All MOD projects implementing this policy can find a list of COIs and the current set of approved data objects on the CVR website.

## Relevant Links

JSP 329 - Information Coherence for Defence - contains the full versions of all of the policies to which this leaflet specifically refers. These may all be accessed via the contents page available [here](#).

For those with a NC3TA account, NATO C3 Technical Architecture is available here. <http://194.7.80.153/website/home.asp?menuid=10>

Office of Public Sector Information - Cabinet Office Legislation is available here. <http://www.opsi.gov.uk/legislation>

e-Government Metadata Standard v 3.1 issued August 2008 is available here. <http://www.govtalk.gov.uk/>

The Freedom of Information Act (2000) is available here. <http://www.opsi.gov.uk/acts/acts2000/20000036.htm>

### [JSP 602 Leaflets](#) (Internet)

JSP 602:1007 Database Services  
JSP 602:1012 Information Interchange Pdf  
JSP 602:1014 Legislation Pdf

A glossary of terms and abbreviations used within this document is available [here](#).

Instructions on "[how to read](#)" a JSP602 leaflet are available here.

## Compliance

Stage	Compliance Requirements
<b>Initial Gate/DP1</b>	JSP329 contains the guidance on information coherence for ALL projects. All MOD projects are expected, as a minimum at initial gate, to submit a formal declaration that they have read and complied with the applicable JSP329 Policy set. The declaration must confirm that they have identified the COI responsible for their area, and sought guidance from the COI as required. Evidence that a Through Life Information Management Plan (TLIMP) is being drafted that covers these requirements should be provided.
<b>Main Gate/DP2</b>	A mature TLIMP should be available. All MOD projects are required to submit a formal declaration that they have read and complied with the full Information Coherence for Defence Policy as set out in JSP329. A typical statement should be included in the TLIMP to confirm that they have engaged with their COI and declared that their CIS development,

	procurement or updating processes can demonstrate how the requirements of the Policy have been complied with.
<b>Release Authority/DP5</b>	<p>MOD Projects (supported by their suppliers) shall provide evidence of their compliance with the relevant JSP329 policies within the System Requirements Document (SRD) and Ministry of Defence Architectural Framework (MODAF) technical views. Evidence of conformance with standards shall be presented; sources of evidence may include:</p> <p>conformance/compliance certificates provided by suppliers (e.g. under type approval or other assessment regimes), demonstrations, inspections analysis, tests carried out by suppliers (e.g. Factory Acceptance Tests) and tests carried out at Defence Test and Reference Facilities. They will also be required to show where any new data entities (a single person, place, or thing about which data can be stored) used within their CIS are registered.</p>