JSP 602 Instruction	1034	**Applicability**	Applications, Infrastructure, Network/Communications, Security
Configuration Identity	Version: 01.02 Amended: 2009-03-02 Reviewed: 2006-06-27	**Epoch Applicability**	2005 - 2009

JSP 602: 1034 - Network Mapping and Configuration Management

Outline

Description: Network Mapping and Configuration Management covers the policy necessary to ensure that MOD networks and infrastructure are properly mapped (i.e. the physical and logical architecture is properly recorded) and that their configuration is fully managed and controlled.

Reasons for Implementation: The MOD Global Information Infrastructure is continuously changing as new systems are added, redundant systems removed and existing systems modified. Network mapping and configuration management is necessary to help minimise the risks to MOD of undesirable and unpredictable performance of the infrastructure. This policy supports the RAP that has been instigated as a means of managing the risks introduced when many systems and services co-exist as part of MOD's infrastructure.

Issues: This policy applies to systems, services and applications during procurement in that their configuration must be known prior to connecting to the MOD infrastructure. However, this policy must also be applied after a system, service or application has entered service as it is equally important that network mapping and configuration management is maintained throughout the CADMID cycle.

Guidance: This policy forms part of the Release Assurance Process covered within JSP 602: 1033 - Release Assurance.

This policy is outside the scope of both the e-GIF and the NC3TA.

Policy

Strategic

1034.01: Network Mapping

1034.01.01 All projects and/or owners of equipment that connect to, are hosted on, or intend to connect to or be hosted on the GII shall declare the following network mapping information:

1034.01.01.01 configuration/build state of all servers.

1034.01.01.02 configuration/build state of all client devices.

1034.01.01.03 configuration/build state of all network and components.

1034.01.01.04 logical and physical views/representations of the equipment configuration and its connection to the GII.

Maintaining an up-to-date map of the GII requires detailed configuration information to be declared.

Comment: This information is required to support network configuration management and maintenance of the network map. Eventually this policy should define the standards covering the notation/presentation of the information, level of detail and the data formats required to load the information into a common repository. This definition work is currently on-going and should be used to update this JSP602 in due course.

1034.02: Installation Configuration Management

1034.02.01 All systems, services or applications joining or being hosted on the GII, being modified or being removed from the GII shall comply with the following:

1034.02.01.01 JSP 480, 5th Edition, Jul 2004 - Defence CIDA Manual of Regulations for Installation of Communications & Information Systems.

Comment: The design rules described in JSP 480 represent 'Commercial Best Practice'. It enshrines the mandatory rules of the IEE Regulations (16th Edition) designed also to take into account the needs of the MOD to make best use of its infrastructure, especially in highly confined operational areas and in the management of classified data. The processes of notification and approval within JSP 480 are mandatory. Design principles may be either mandatory or for guidance depending on the context to which they apply. Those proposals that are fully compliant with such principles from the outset can be expected to gain CIDA consent without request for amendment. CIDA and its agents operate a "Service Level" concept whereby all sites and sub-sites are controlled to a level commensurate with the operational importance of the site, both militarily and commercially, and the rate of change experienced on the site. High risk = High control.

1034.02.01.02 JSP440 Issue 3 Amdt. 2, April 2004 - Defence Manual of Security: part 7 Physical and Environmental, part 8 Communications and Information Systems.

JSP 480 and JSP 440 are the extant policy documents that cover the configuration control and management of GII components.

Deployed

As for Strategic domain.

Tactical
As for Strategic domain.

Remote
As for Strategic domain.

Responsibility for Implementing the Policy

Implementation of this policy shall be the responsibility of all IPTs (and their suppliers) that provide systems, services or applications that connect to, or are hosted on, the GII.

Procedure

Network Mapping: Configuration management of the network is the responsibility of DCSADSD- Architecture. The information produced in response to this policy must be submitted to DCSA-DSD-Architecture Hd, Basil Hill Site, Park Lane, Corsham, Wilts. SN13 9NR.

Installation Configuration Management: The procedures for implementing the configuration management of MOD installations requires the projects to use the Defence CIDA organisation. This is based within the Directorate of Engineering, Interoperability and Information Services located at RAF Henlow and Blandford Camp. It comprises 4 sections providing a CIDA service, primarily on a geographic basis, with responsibilities as follows:

- CM-CIDA1 (Henlow) Policy, Purple Sites, sites within M25, commercial organisations, Italy, Middle East, Africa, Ascension and TCW/30 Sig Regt;

- CM-CIDA2 (Blandford) Sites south & west of M4-M25-M23, NI, Germany, Balkans, Cyprus and FI;

- CM-CIDA3 (Henlow) Other sites in UK, N&S America, Gibraltar and all special sites;

- CM-CIDA4 (Henlow) Radio site clearance and safeguarding including cartography. RAF owned ducts.

Every MOD site must have a SCIDA who must be informed and provide agreement to any change that is proposed for the site. Agreement shall also be sought and obtained from the SCIDA that the final installation is in accordance with the original proposal and is of satisfactory status. Designers and end users should be aware that agreement by CIDA to either the design or completed installation does not imply a guarantee of design functionality.

Relevant Links

JSP 602: 1033 - Release Assurance

AMS guidance JSP 480 - CIDA Manual of Regulations for Installation of Communications & Information Systems can be found here (restricted site only).
(http://www.ams.mod.uk/ams/default.htm)

AMS guidance on JSP 440 can be found here (restricted site only).
(http://www.ams.mod.uk/ams/default.htm)

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
Initial Gate/DP1	MOD Projects shall submit a formal declaration that they have read and understood the policy and sought guidance from the SME(s).
Main Gate/DP2	MOD Projects shall provide documentation defining at a high level their configuration management processes that relate to this policy.
Release Authority/DP5	MOD Projects (supported by their equipment suppliers) shall provide documentation defining in detail the configuration management processes that relate to this policy as evidence of their compliance with it. They shall also provide documented configuration information for their system(s), service(s) and/or application(s) as demanded by this policy.