JSP 602 Instruction	1013	**Applicability**	Applications, Data/Information, Infrastructure, Network/Communications
Configuration Identity	Version: 01.02 Amended: 2009-03-02 Reviewed: 2006-06-21	**Epoch Applicability**	2005 - 2009

JSP 602: 1013 - Internetworking

Outline

Description: Internetworking defines the protocols required to provide a basic packet-switched, routed, reliable network across the GCN and between elements of the GCN and other (external) networks.

Reasons for Implementation: The delivery of a standardised, reliable data service is fundamental to achieving interoperability between component networks and systems within MOD. It is also a critical part of achieving any level of automated information exchange with other organisations.

Issues: For reasons of efficiency, not all systems will implement the standards identified in this policy internally (e.g. satellite communications systems). However, all systems and support components shall support them at their respective boundaries.

Guidance: This policy is compliant with the e-GIF. The e-GIF does not address private-to-public IP address translation policy. This policy is compliant with the NC3TA.

Policy

Strategic

1013.01: Internetworking

1013.01.01 All systems and networks shall support the following Internetworking standards:

1013.01.01.01 IPv4 (RFC791:1981, 792:1981, 894:1984, 919:1984, 922:1984, 1112:1989)

1013.01.01.02 TCP (IETF STD 7:1981)

1013.01.01.03 UDP (IETF STD 6:1980)

These are the ubiquitous standards.

Comment: IP addressing policy is contained in JSP602: 1023 - Domain Naming and IP Addressing.

1013.02: Private Address Ranges and Address Translation

1013.02.01 All systems using private address ranges shall implement address translation at their boundaries using standards as follows:

1013.02.01.01 NAT (RFC 3022:2001)

This service is necessary when joining networks together or sharing services between networks and one of the networks is running a private address space. NAT has the effect of extending the IPv4 address space and is commonly supported in commercial routers.

1013.02.02 Private address ranges shall not be used unless specifically authorised by DINSA.

Comment: No Private IP addresses must ever be routed over public networks if this is exposed to the routing network. Neither should Private IP addresses be advertised as service points or routes.

1013.03: Internet Protocol version 6

1013.03.01 All new network implementations or technology refresh points shall implement components that can host both IPv4 and v6 address space. These devices shall also be capable of presenting a conversion service at their boundary.

1013.03.01.01 IPv6 (RFC 2460:1998, 2461:1998, 2462:1998, 2463:1998, 2464:1998, 2373:1998, 2374:1998, 2375:1998, 2710:1999, 3513:2003)

This is to ensure that a future move to IPv6 can be implemented and managed more easily.

Comment: The move to IPv6 must be planned and implemented such that the impact on existing systems in minimised. Early preparation for its implementation will help prevent costly upgrades in the future.

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 MOD Projects (and their suppliers) that provide or use IP-based services within the GII.

Procedure

Not Applicable.

Relevant Links

JSP602: 1023 - Domain Naming and IP Addressing

Details of those RFCs listed can be found here. (http://www.rfc-editor.org/rfcsearch.html)

Details of IETF standards listed can be found here. (http://www.apps.ietf.org/rfc/stdlist.html)

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 reference in their SRD (and MODAF technical views) the specific policy elements contained within this leaflet that are applicable to the system, equipment or application they are procuring or updating.
Release Authority/DP5	MOD Projects (supported by their equipment suppliers) shall provide evidence of their compliance with the elements of this policy defined within the SRD (and MODAF technical views). Evidence of conformance with standards shall be presented; sources of evidence may include: conformance/compliance certificates provided by equipment suppliers (e.g. under type approval or other assessment regimes), demonstrations, inspection, analysis, tests carried out by suppliers (e.g. Factory Acceptance Tests) and tests carried out at Defence Test and Reference Facilities.