



**Joint Service Publication
604
Network Joining Rules**

MINISTRY OF DEFENCE

Issue 1.1
May 2009

UNCONTROLLED WHEN PRINTED

This policy has been equality and diversity impact assessed in accordance with Departmental policy. This resulted in a Part 1 screening only completed (no direct discrimination or adverse impact identified)

DOCUMENT HISTORY SHEET

ISSUE NUMBER / AUTHOR	DESCRIPTION OF MAJOR CHANGES	DATE
Issue 0.1 ISS Sols-C4 Tech Arch 1	Initial draft issue produced by JSP 604 Sponsor (DES D ISS).	23/02/2009
Issue 0.2 – 0.4 ISS Sols-C4 Tech Arch 1	Incorporation of initial comments from DES D ISS SvcOps.	10/03/2009
Issue 0.5 ISS Sols-C4 Svc Arch 1 ISS Sols-Int SRA Hd	Update of Network Joining Rules and Introduction.	01/04/2009
Issue 0.6 ISS Sols-C4 Svc Arch 1 ISS Sols-Int SRA Hd	Incorporation of EDIAT Statement	01/04/2009
Issue 0.7 ISS Sols-C4 Svc Arch 1 ISS Sols-Int SRA Hd	Minor grammatical errors removed	02/04/2009
Issue 0.8 ISS Sols-C4 Svc Arch 1 ISS Sols-Int SRA Hd	Incorporation of comments from CIO-XStrat	06/04/2009
Issue 1.0 ISS Sols-C4 Svc Arch 1 ISS Sols-Int SRA Hd	Formal issue of JSP 604 approved by JSP 604 Owner (Defence CIO).	07/04/2009
Issue 1.1 ISS Sols-C4 Svc Arch 1 ISS Sols-Int SRA Hd	Changes to JSP reference and broken hyperlink under Rule 8. Correction of email contact details due to role changes	08/08/2009

CONTENTS

DOCUMENT HISTORY SHEET _____	ii
CONTENTS _____	iii
Introduction _____	1
Background _____	1
Ownership and Authority _____	1
Applicability _____	1
Network Joining Rules Risk Balanced Cases _____	2
Roles and Responsibilities _____	3
References _____	4
Network Joining Rules _____	6
Rule 1: Maximise Benefit to the Enterprise _____	6
Rule 2: Lead Business Architect, Technical Architect and Integrator Appointments _____	8
Rule 3: Configuration Management / Co-ordinating Installation Design Authority (CIDA) _____	9
Rule 4: Information Assurance _____	10
Rule 5: Computer Network Defence (CND) _____	10
Rule 6: Patch Management _____	11
Rule 7: Security Accreditation _____	11
Rule 8: Systems Safety _____	12
Rule 9: Performance Management _____	13
Rule 10: Bandwidth Utilisation _____	14
Rule 11: Packet Switched Service _____	14
Rule 12: Spectrum Management _____	15
Rule 13: Messaging _____	15
Rule 14: Naming & Addressing _____	16
Rule 15: Directories _____	16
Rule 16: Equipment Support _____	17
Rule 17: Service Continuity Management _____	17

INTRODUCTION

BACKGROUND

1. This Defence Chief Information Officer (CIO) owned Joint Service Publication (JSP) has been developed to define the irreducible minimum set of rules that are to be applied to all systems interacting with the Department's current and planned Communication and Information Systems (CIS).
2. MoD requires a flexible, cohesive and interoperable network of systems to support the delivery of Network Enabled Capability (NEC). As part of the JSP 600 series for MoD CIS Policy and Assurance Process, JSP 602 details the technical standards required for CIS Interoperability. JSP 604 does not duplicate those standards but identifies those that are applicable to projects that have an interaction with the Department's CIS networks.
3. JSP 604 (known as 'Network Joining Rules') will assist decision makers at all levels in understanding the risk and impact of their decisions and play a 'protecting' role in ensuring that existing CIS capability continues to satisfy required service levels through life. This first issue of JSP 604 defines rules for what is the acceptable conduct of a 'Good Neighbour' on CIS Networks. The evolution of these rules will be against increasing levels of interoperability and co-existence thus supporting the successful delivery of NEC. This document will initially be reviewed on a three monthly basis.

OWNERSHIP AND AUTHORITY

4. The Defence CIO, as owner of the JSP 600 series for MoD CIS Policy and Assurance has approved the issue of this document. JSP 604 is sponsored, controlled and maintained by Director Information Systems and Services (D ISS). The document is designed to be adaptive and will evolve in accordance with the direction given by the CIO Systems Direction Group whose Defence Management Board (DMB) endorsed role is to identify where accelerated improvements in existing programmes can be made by applying new policies, architectures, standards or engineering approaches. The next review is scheduled for July 2009.

APPLICABILITY

5. JSP 604 is mandated by the Defence CIO for all projects and/or programmes across Defence¹ that constitute or interact with current and programmed Departmental CIS. D ISS, as the document's sponsor, is responsible for the content, publication and management of JSP 604.
6. In accordance with the ethos of Through Life Capability Management, projects are required to apply the rules throughout the project and/or programme's acquisition life-cycle. Traditionally, functional assurance is only primarily required at the Initial and Main Gate decision points. These rules shall be applied as follows:

¹ This extends to all MoD organisations including Trading Funds and Agencies

- a. Initial Gate: Projects and/or programmes are required to provide a statement to the effect that they understand the requirements of JSP 604 as applied to their case and a broad intent as to how they intend to satisfy the requirements through life.
- b. Preliminary Design Review (PDR) and Main Gate: Projects and/or programmes are required to provide broad evidence (usually as part of the preliminary design review) that they have developed appropriate plans to demonstrate compliance with the requirements of JSP 604. For CIS services that are constituted from more than one CIS component² there is a requirement that the PDR is signed off by all CIS providers.
- c. Critical Design Review: Projects and/or programmes are required to provide specific plans as to how they will demonstrate compliance with the requirements of JSP 604.
- d. Prior to IOC, Full Scale Production or Deployment: Projects and/or programmes are required to provide specific interpreted evidence as to how they have demonstrated compliance with the requirements of JSP 604.
- e. Through Life Changes: Projects and/or programmes are required to continue to apply the JSP 604 Network Joining Rules through life and there is a requirement to ensure that any upgrades or changes (be these part of an incremental acquisition strategy or in-service changes that have an impact on the network) also comply with the Network Joining Rules extant at that time.

7. In the first instance, the rules will be applied by D ISS (Head Solutions) staffs to projects and/or programmes with a CIS element or reliance on the Department's CIS. Responsibility lies with individual projects and/or programmes to engage with the Service Release Team within D ISS (Head Solutions), through the D ISS 'Requirements Front Door'³, to establish the applicability of each Network Joining Rule.

NETWORK JOINING RULES RISK BALANCED CASES

8. Exceptionally, for a project and/or programme where a deviation from the rules is identified, a '*Network Joining Rules Risk Balanced Case*' will need to be made by the project sponsor to the CIO for consideration⁴. The risk balanced case will, in the first instance, need to be submitted to the Service Release Team for consideration. All cases involving security considerations must have a clear recommendation from DSSA. The process is as follows:

- a. The project sponsor is to develop the risk balanced case.

² For example an application service delivered by an organisation external to D ISS that is dependent on the D ISS Infrastructure and/or Network services

³ In accordance with the D ISS 'Requirements Coherence Process'

⁴ Risk Balance Method guidance is available in JSP 440 Supplement 12

- b. The risk balanced case is to be submitted to the Service Release Team for consideration and discussion with the project/programme's stakeholders.
- c. If an exception is agreed as appropriate the risk balanced case will be staffed to D ISS (Head Solutions) acting as the MoD Chief Technology Officer (CTO⁵) for CIS and to D ISS acting as the DE&S CIO.
- d. For projects and/or programmes that sit outside of DE&S, the sponsor is to additionally consult with their TLB CIO (where one is established) during the development of the risk balanced case.
- e. If the risk balanced case is not agreed as per sub para c, then it shall be escalated to the Defence CIO.

ROLES AND RESPONSIBILITIES

9. Comments or questions on the content of this Joint Service Publication should be directed to:

Address:	DE&S D ISS Sols-Architect Deputy Head Room F101 Building H4 Copenacre Site Corsham Wiltshire SN13 9NR
MoD VPN Tel:	(9) 67700493
PSTN Tel:	0306 7700496
MoD VPN Fax:	(9)4382 6912
PSTN Fax	01225 846912
SMTP (Internet) e-mail:	DESISSSols-ArchGroupMail@mod.uk

10. Comments or questions on the application of this Joint Service Publication should be directed to:

Address:	DE&S D ISS Sols-Integration Service Release Authority Room F101 Building H4 Copenacre Site Corsham Wiltshire SN13 9NR
MoD VPN Tel:	(9) 67700554

⁵ The MoD CTO for CIS is the owner of technical risk for the network

PSTN Tel:	0306 7700554
MoD VPN Fax:	(9)4382 6912
PSTN Fax	01225 846912
SMTP (Internet) e-mail:	DESISSSols-IntSRAGroupMail@mod.uk

11. Comments or questions on the D ISS Solutions Requirements Front Door Process should be directed to:

Address:	DES D ISS Sols-Requirements B Hd Room F001 Building H4 Copenacre Site Corsham Wiltshire SN13 9NR
MoD VPN Tel:	(9)4382 6940
PSTN Tel:	01225 846940
MoD VPN Fax:	(9)4382 6912
PSTN Fax	01225 846912
SMTP (Internet) e-mail:	DESISSSols-ReqB-AsstHd@mod.uk

12. JSP 604 is available for download from the Defence Intranet by clicking [here](#).

REFERENCES

13. In applying the Network Joining Rules, the project and/or programme should take cognisance of the following CIS policy, rules or guidance:

- a. Deployed Technical Architecture
- b. DII Application Development Guide
- c. Global Information Infrastructure (GII) Architecture
- d. Interoperability for Communication and Information Systems
- e. Ministry Of Defence Architecture Framework (MODAF)
- f. MoD Service Oriented Architecture (SOA) Handbook
- g. Service Release Handbook
- h. JSP 440: The Defence Manual of Security (Part 8: Communication and Information Systems Security)

- i. JSP 457: Defence Manual of Interoperable Core Network Technologies
- j. JSP 480: Defence Co-ordinating Installation Design Authority (CIDA) Manual of regulations for installation of communication & information systems
- k. JSP 600: MoD CIS Policy and Assurance Process.
- l. JSP 602 Leaflets: Information Coherence Directions and Guidance
- m. JSP 777: NEC Handbook

NETWORK JOINING RULES

<u>RULE 1: MAXIMISE BENEFIT TO THE ENTERPRISE</u>	
Statement:	Delivery and development decisions are made to provide maximum benefit to the enterprise as a whole.
Rationale:	This principle embodies "service above self". Decisions made from an enterprise-wide perspective have greater long-term value than decisions made from any particular organisational perspective. Maximum return on investment requires decision makers to adhere to enterprise-wide drivers and priorities. No minority group will detract from the benefit of the whole. However, this principle will not preclude any minority group from getting its job done.
Implications:	<ol style="list-style-type: none">1. Achieving maximum enterprise-wide benefit will require changes in the way we plan and manage our activities. Technology alone will not bring about this change.2. Some organisations may have to concede their own preferences for the greater benefit of the entire enterprise.3. Development priorities must be established by the entire enterprise for the entire enterprise.4. Reusable components shall be shared across organisation and project boundaries.<ol style="list-style-type: none">a. Technology Architecture – Infrastructure. Defence Information Infrastructure (DII) services shall be progressively adopted as the delivery mechanism for core information services⁶ supporting the MoDs business and administration, in addition to the joint and combined planning at strategic and operational levels.b. Technology Architecture – Network. Defence Fixed Telecommunications System (DFTS) services shall be used for all telephony and WAN services within the UK and UK bases in 14 countries including Germany and Cyprus until 31 July 2012 as defined within the DFTS contract.c. Technology Architecture – Network. SkyNet 5 services shall be used for all military satellite services worldwide.d. Technology Architecture – Network. NATO Allied Long-Lines Agency (NALLA) services shall be used for the provision of terrestrial International Private Leased Circuits (IPLCs) WAN services outside the contractual remit of DFTS.e. Technology Architecture – Network. Defence High Frequency Communications Service (DHFCS) and Very Low Frequency Received Signal Service (VLF RSS) services shall be used for strategic long haul radio (VLF, LF, HF) services.f. Technology and Application Architecture – The Defence CIS SPOC shall be used for all first line CIS service desk support calls.5. Individual projects should pursue initiatives which conform to the MoD GII Architecture and standards as described by CIO, DES SEIG, DES ISS Sols-Architect and the priorities established by the enterprise.

⁶ Examples of DII core services include: User Access Devices (UADs), e-mail, office automation, Electronic Document Recording and Management (EDRM), application hosting, directories, messaging, web services and browsing.

Implications (continued)	<p>6. Projects must justify why they cannot utilise existing CIS services to meet their requirements. Where it is not intended to use existing services, the Business Case and Architecture documentation must set out the rationale for the decision, the resources allocated to the provision of the alternate CIS services and the arrangements to address conformance with existing CIS services. Exceptionally, for a MoD Project where significant deviation from the rules is identified, there will be an escalation route to the Defence CIO to seek a waiver to introduce new services.</p> <p>As needs arise, priorities must be adjusted by a suitable forum, such as the Joint Capability Board (JCB) or Directors of Equipment Capability (DECs) supported by Capability Management Groups (CMGs) and their subordinate Capability Planning Groups (CPGs) & Programme Boards (PBs)</p>
Architecture Applicability:	<p>Business Architecture Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks</p>
Policy References:	<p>DG Info/8/5/1 (107/05) Convergence to Defence Information Infrastructure (DII) Core Services, 10 Aug 05.</p>
Subject Matter Expertise POCs:	<p>DE&S D ISS Solutions-Architect Deputy Head DE&S D ISS Applications Services Team DE&S D ISS Infrastructure Services Team DE&S D ISS Networks Services Team</p>

<u>RULE 2: LEAD BUSINESS ARCHITECT, TECHNICAL ARCHITECT AND INTEGRATOR APPOINTMENTS</u>	
Statement:	All systems shall appoint a lead Business Architect, lead Technical Architect and lead Systems Integrator.
Rationale:	<p>Experience has demonstrated that projects and/or programmes without such appointments face increased technical and project risks resulting in a failure to deliver outcomes within the agreed time, cost and performance envelope.</p> <p>The lead Business Architect shall have responsibility for delivering the strategy, governance, organisation and key business processes for the capability.</p>
Implications:	<p>Verification & Validation Compliance:</p> <ol style="list-style-type: none"> 1. Evidence is to be provided that the required appointments have been made and that the personnel are active participants in the delivery of the capability. 2. At decision points (that include but are not limited to Initial Gate, Preliminary Design Review, Main Gate, Interoperability Design Review, Critical Design Review, Initial Operating Capability, Full Operating Capability etc), the project shall provide evidence that they have developed appropriate plans to demonstrate compliance with the requirements of JSP 604 through life. There is an expectation that the evidence will have matured between each decision point. For CIS services that are constituted from more than one CIS component⁷ there is a requirement that the PDR is signed off by all dependant CIS providers.
Architecture Applicability:	<p>Business Architecture</p> <p>Information Systems Architecture – Data</p> <p>Information Systems Architecture – Applications</p> <p>Technology Architecture – Infrastructure</p> <p>Technology Architecture – Networks</p>
Policy References:	<p>ITIL V3</p> <p>MODAF</p> <p>TOGAF 9</p>
Subject Matter Expertise POCs:	<p>Chief Information Officer (CIO)</p> <p>DE&S D ISS Solutions-Architect Deputy Head</p> <p>DE&S D ISS Solutions-Integration Deputy Head</p>

⁷ For example an application service delivered by an organisation external to D ISS that is dependent on the D ISS infrastructure and/or network services.

<u>RULE 3: CONFIGURATION MANAGEMENT / Co-ORDINATING INSTALLATION DESIGN</u> <u>AUTHORITY (CIDA)</u>	
Statement:	<p>Before connection to the GII, all systems must have an Asset Management and Configuration Management process in place.</p> <p>All networks and systems must provide and maintain a full documentation set and topology under configuration control through life.</p> <p>Provide physical and environmental CIS design and installation documentation, appropriate to the required level of confidentiality, integrity and availability. This shall include, but not be limited to, the appropriate level of resilient electrical CIS HVAC and power requirements.</p>
Rationale:	Due to time constraints it is not possible to define the rationale in this issue of JSP 604. It will be defined in a later issue.
Implications:	<p>Verification & Validation Compliance:</p> <ol style="list-style-type: none"> 1. Projects providing network infrastructure must obtain CIDA design conformance approval before proceeding with installations. 2. Projects must demonstrate how they will carry out configuration management and how they will make this information available to the D ISS Global Operations Security Control Centre (GOSCC).
Architecture Applicability:	<p>Technology Architecture – Infrastructure</p> <p>Technology Architecture – Networks</p>
Policy References:	<p>JSP 480</p> <p>ITIL v3</p> <p>CBMJ6 Executive Group Requirements (for power)</p>
Subject Matter Expertise POCs:	<p>DE&S D ISS CM CIDA</p> <p>DSSA</p> <p>DE&S D ISS Service Operations</p>

<u>RULE 4: INFORMATION ASSURANCE</u>	
Statement:	Any system connecting to the GII must have an independent computer security audit undertaken.
Rationale:	Due to time constraints it is not possible to define the rationale in this issue of JSP 604. It will be defined in a later issue.
Implications:	Validation & Verification Compliance: Projects shall provide assurance that all recommendations as a result of an audit have/will be implemented.
Architecture Applicability:	Business Architecture Information Systems Architecture – Data Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks
Policy References:	JSP 440
Subject Matter Expertise POCs:	DE&S D ISS Service Operations DIO

<u>RULE 5: COMPUTER NETWORK DEFENCE (CND)</u>	
Statement:	CND monitoring facilities must be included in any network design in order to meet Enhanced CND requirements.
Rationale:	Due to time constraints it is not possible to define the rationale in this issue of JSP 604. It will be defined in a later issue.
Implications:	Verification & Validation Compliance: Assurance that the network design includes facilities to carry out the CND function and that the results can be made available to the D ISS Global Operations Security Control Centre (GOSCC).
Architecture Applicability:	Business Architecture Technology Architecture – Infrastructure Technology Architecture – Networks
Policy References:	
Subject Matter Expertise POCs:	DE&S D ISS Service Operations DE&S D ISS Network Services Team (ECND Project)

<u>RULE 6: PATCH MANAGEMENT</u>	
Statement:	All systems that involve software components shall have a security patch management policy and set of supporting procedures in place. All software patches and software upgrades released to correct vulnerabilities present on MoD CIS must be applied (including testing and integration) within one month of publication unless otherwise directed by MODCERT.
Rationale:	To ensure that CIS are not made vulnerable to attack through use of known weaknesses.
Implications:	Validation & Verification Compliance: Projects shall demonstrate how they will carry out availability management, including software patching.
Architecture Applicability:	Business Architecture Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks
Policy References:	JSP 440 ITIL v3
Subject Matter Expertise POCs:	DE&S D ISS Service Operations

<u>RULE 7: SECURITY ACCREDITATION</u>	
Statement:	Any system connecting to the GII must be accredited by DSSA prior to Service Release.
Rationale:	Due to time constraints it is not possible to define the rationale in this issue of JSP 604. It will be defined in a later issue.
Implications:	Verification & Validation Compliance: 1. It is essential whenever initiating any connection to the GII that DSSA is contacted at the earliest opportunity and a dialogue initiated with the system accreditor. For all new connecting systems without an accreditor DSSA will be allocate one at this stage. 2. In order to join - All systems will have interim/full accreditation or hold a valid risk balance case signed off by the relevant SIRO.
Architecture Applicability:	Business Architecture Information Systems Architecture – Data Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks

Policy References:	SPF JSP 440 JSP 480
Subject Matter Expertise POCs:	DSSA-DDAcc

<u>RULE 8: SYSTEMS SAFETY</u>	
Statement:	Assurance shall be provided that appropriate safety cases are produced by suitably qualified experienced personnel for all CIS applications, infrastructure and networks prior to service release.
Rationale:	Ensure that, where necessary, a systems safety case has been produced in order to meet legal requirements.
Implications:	Verification & Validation Compliance: Applications, Infrastructure & Networks have to provide evidence that adequate safety cases have been produced in order to comply with requirements in legislation, MoD Policy & guidance including the Acquisition Safety & Environmental System (ASEMS).
Architecture Applicability:	Business Architecture Information Systems Architecture – Data Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks
Policy References:	JSP 815 Acquisition Safety & Environmental Management System (ASEMS)
Subject Matter Expertise POCs:	DE&S D ISS Programmes-C4 Safety and Environment E-mail: DES ISS Sols-C4 Safety and Env1 Tel: (9)4382 6096 DE&S D S&E Safety & Environmental Protection (CESO)

<u>RULE 9: PERFORMANCE MANAGEMENT</u>	
Statement:	<p>All projects will have an affect on CIS capacity and must identify the extent of that effect and ensure that capacity and availability of existing CIS capabilities are maintained following implementation.</p> <p>All projects must ensure that they comply with technical performance management requirements as laid down by the network owner (this is to include those capabilities that constitute the network).</p>
Rationale:	<p>ITIL v3 defines Performance Management as the Process responsible for day-to-day Capacity Management Activities. These include Monitoring, Threshold detection, Performance analysis and Tuning, and implementing Changes related to Performance and Capacity.</p> <p>ITIL v3 defines Capacity Management as the Process responsible for ensuring that the Capacity of IT Services and the IT Infrastructure is able to deliver agreed Service Level Targets in a Cost Effective and timely manner. Capacity Management considers all Resources required to deliver the IT Service, and plans for short, medium and long-term Business Requirements. Capacity Planning is the activity within Capacity Management responsible for creating a Capacity Plan.</p> <p>Projects and/or programmes shall characterise their application(s) performance on a representative test environment prior to release.</p>
Implications:	<p>Validation & Verification Compliance:</p> <ol style="list-style-type: none"> 1. Projects shall demonstrate that proposed changes to an existing service will not adversely affect the performance of existing CIS capabilities. If they do, then they must show that provision has been made to cater for the increase. 2. Projects shall demonstrate that they are able to pass the agreed set of technical performance management datasets to the network owner.
Architecture Applicability:	<p>Business Architecture</p> <p>Information Systems Architecture – Applications</p> <p>Technology Architecture – Infrastructure</p> <p>Technology Architecture – Networks</p>
Policy References:	ITIL v3
Subject Matter Expertise POCs:	<p>DE&S D ISS Service Operations</p> <p>DE&S D ISS Integration Continual Service Improvement</p>

<u>RULE 10: BANDWIDTH UTILISATION</u>	
Statement:	Any application that plans to operate over the GII must provide qualified information on the required bandwidth before connecting so that capacity planning can be undertaken.
Rationale:	Due to time constraints it is not possible to define the rationale in this issue of JSP 604. It will be defined in a later issue.
Implications:	Validation & Verification Compliance: Projects shall ensure that once the system is established in a representative test environment, the actual bandwidth shall be established and confirmed against representative use cases.
Architecture Applicability:	Business Architecture Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks
Policy References:	JSP 602: 1030 – Wide Area Bandwidth MODAF View SV-7: Resource Performance Parameter
Subject Matter Expertise POCs:	DE&S D ISS Solutions-Integration Service Release Authority E-mail: DES ISS Sols-Int SRA GroupMail (MULTIUSER)

<u>RULE 11: PACKET SWITCHED SERVICE</u>	
Statement:	All systems will be IPv4 based both internally and at the gateways. All equipment purchased shall be IPv6 capable.
Rationale:	Due to time constraints it is not possible to define the rationale in this issue of JSP 604. It will be defined in a later issue.
Implications:	Validation & Verification Compliance: Projects shall submit a formal declaration that they comply with MoD policy and have sought guidance from the SME.
Architecture Applicability:	Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks
Policy References:	JSP 602: 1013 – Internetworking JSP 457
Subject Matter Expertise POCs:	DE&S D ISS Solutions-Architect Deputy Head

<u>RULE 12: SPECTRUM MANAGEMENT</u>	
Statement:	The system shall not cause unacceptable levels of RF interference to existing systems.
Rationale:	Due to time constraints it is not possible to define the rationale in this issue of JSP 604. It will be defined in a later issue.
Implications:	Verification & Validation Compliance: The Defence E3A organisation must approve any system that utilises electromagnetic transmissions.
Architecture Applicability:	Technology Architecture – Infrastructure Technology Architecture – Networks
Policy References:	JSP 602:1038 JSP 480
Subject Matter Expertise POCs:	DE&S D S&E SEIG Defence E3A

<u>RULE 13: MESSAGING</u>	
Statement:	All low, medium and high grade messaging systems shall utilise SMTP.
Rationale:	Allows common standards for interoperability. SMTP is the de facto international standard.
Implications:	Verification & Validation Compliance: Projects shall submit a formal declaration that they comply with MoD policy and have sought guidance from the SME.
Architecture Applicability:	Information Systems Architecture – Data Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks
Policy References:	JSP 602: 1016 – Messaging Services JSP 457
Subject Matter Expertise POCs:	DE&S D ISS Solutions-Architect Deputy Head DE&S D ISS DII Engineering Management

<u>RULE 14: NAMING & ADDRESSING</u>	
Statement:	All systems shall comply with the Defence Naming and Addressing Standards.
Rationale:	Due to time constraints it is not possible to define the rationale in this issue of JSP 604. It will be defined in a later issue.
Implications:	Verification & Validation Compliance: Projects shall submit a formal declaration that they comply with MoD policy and have sought guidance from the SME.
Architecture Applicability:	Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks
Policy References:	JSP 602:1023 JSP 457
Subject Matter Expertise POCs:	DE&S D ISS Solutions-Architect Deputy Head

<u>RULE 15: DIRECTORIES</u>	
Statement:	Any solution that will be required to share or update information in the UK or with Allies and NATO should utilise the Defence X.500 schema.
Rationale:	Due to time constraints it is not possible to define the rationale in this issue of JSP 604. It will be defined in a later issue.
Implications:	Verification & Validation Compliance: Projects shall submit a formal declaration that they comply with MoD policy and have sought guidance from the Directories Steering Board.
Architecture Applicability:	Business Architecture Information Systems Architecture – Data Information Systems Architecture – Applications Technology Architecture – Infrastructure
Policy References:	JSP 602:1009 JSP 457
Subject Matter Expertise POCs:	DE&S D ISS Solutions-Architect Deputy Head DE&S D ISS DII Engineering Management

<u>RULE 16: EQUIPMENT SUPPORT</u>	
Statement:	Detailed Equipment Support and Service Support policy and procedures shall be in place.
Rationale:	Due to time constraints it is not possible to define the rationale in this issue of JSP 604. It will be defined in a later issue.
Implications:	Verification & Validation Compliance: The Project shall demonstrate how the system will be supported.
Architecture Applicability:	Business Architecture Information Systems Architecture – Data Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks
Policy References:	ITIL v3. Acquisition Operating Framework
Subject Matter Expertise POCs:	DE&S D ISS Service Operations

<u>RULE 17: SERVICE CONTINUITY MANAGEMENT</u>	
Statement:	Projects shall demonstrate how services will be maintained in the event of a major incident.
Rationale:	Due to time constraints it is not possible to define the rationale in this issue of JSP 604. It will be defined in a later issue.
Implications:	Verification & Validation Compliance: Projects must demonstrate how their system will be maintained in the event of a major incident.
Architecture Applicability:	Business Architecture Information Systems Architecture – Data Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks
Policy References:	ITIL v3
Subject Matter Expertise POCs:	DE&S D ISS Service Operations