



**Joint Service Publication
JSP 604
Network Joining Rules**

MINISTRY OF DEFENCE

Issue 2
June 2010

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	08/05/2009
Issue 2.0 ISS Sols-C4 Arch-AIT1 ISS Sols-C4RPM-SRA AsstHd	<ol style="list-style-type: none"> 1. Restructuring of the document and inclusion of appropriate test requirements. 2. Renumbering of rules to reflect changes and amendments 3. Document upissued to version 2 following internal staffing (of draft versions 2.1 to 2.4) 	09/06/2010

CONTENTS

Document History Sheet _____	ii
Contents _____	iii
Introduction _____	1
Background _____	1
Ownership and Authority _____	1
Applicability _____	1
Network Joining Rules Risk Balanced Cases _____	4
Roles and Responsibilities _____	5
References _____	6
Network Joining Rules _____	8
Rule 1: Maximise Benefit to the Enterprise _____	8
Rule 2: Lead Business Architect, Technical Architect and Integrator Appointments _____	10
Rule 3: Coordinating Installation Design Authority (CIDA) _____	11
Rule 4: Vulnerability Assessment _____	12
Rule 5: Quality of Service _____	14
Rule 6: Systems Safety _____	14
Rule 7: Integrated Network Management _____	16
Rule 8: Network Resource Utilisation _____	16
Rule 9: Internet Protocol (IP) and Domain Name System (DNS) _____	18
Rule 10: Electromagnetic Environmental Effects _____	19
Rule 11: Messaging _____	19
Rule 12: Codes of Connection _____	20
Rule 13: Electronic Directory Services _____	21
Rule 14: Equipment Support _____	21
Rule 15: Service Continuity Management _____	22
Proposed Network Joining Rules _____	24

INTRODUCTION

BACKGROUND

1. This Defence Chief Information Officer (CIO) owned Joint Service Publication (JSP) has been developed to define the irreducible minimum set of network joining rules that are to be applied to all systems either funded by or interacting with the Department's current and planned Communication and Information Systems (CIS), here after referred to as the 'network'.

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 policies and standards required for CIS Interoperability which will be revised and re-written as a set of rules and incorporated into the SOSA Rulebook. JSP 604 does not duplicate those rules but identifies those that are applicable to projects that have an interaction with the network.

3. JSP 604 (known as the '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 second 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 continue to be reviewed on a regular 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 Board (DB) 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 December 2010.

APPLICABILITY

5. JSP 604 is mandated by the Defence CIO for all projects and/or programmes across Defence¹ that are funded by the Department, constitute or interact with current and programmed Departmental CIS; this includes Urgent Operational Tasks and Requirements. 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

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

the Initial and Main Gate decision points. The JSP 604 rules shall be applied as follows:

- a. Initial Gate: Projects and/or programmes are required to provide a statement to the Service Release Authority 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 to the Service Release Authority 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 to the Service Release Authority 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 to the Service Release Authority as to how they have demonstrated compliance with the requirements of JSP 604. Until formal approval has been granted the capability may NOT join the network.
- e. Through Life Changes: Projects and/or programmes are required to continue to apply the JSP 604 Network Joining Rules through-life. 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. In accordance with DE&S Standing Instruction 21, this shall be reflected in the Through Life Investment Assurance Plan.

7. At defined decision points³ 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 component⁴ there is a requirement that the PDR is signed off by all dependant CIS providers.

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 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

⁴ 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.

8. 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 '[Customer Portal](#)⁵', to establish the applicability of each Network Joining Rule.

9. Whilst Project Teams may choose to delegate responsibility for the provision of evidence, overall responsibility shall rest with the Project Team to present its case to the Service Release Authority to demonstrate compliance with this JSP.

INTRODUCTION OF JSP604 VERSION 2 CHANGES

10. Version 2 of JSP 604 has introduced a number of changes, these are summarised in the table below.

11. Projects shall apply JSP 604 Version 2 from the date of its publication. Those projects that have already engaged with the D/ISS Service Release Authority and have been applying an earlier version of JSP 604 may continue to do so, although it may be in their interests to adopt this new version. Their ongoing engagement with the Service Release Authority will address this.

SERIAL	VERSION 1.1 RULE	VERSION 2 MAPPING	COMMENTS
1.	Rule 1: Maximising Benefit to the Enterprise	Rule 1: Maximising Benefit to the Enterprise	None
2.	Rule 2: Lead Business Architect, Technical Architect and Integrator Appointments	Rule 2: Lead Business Architect, Technical Architect and Integrator Appointments	None
3.	Rule 3: Configuration Management / Co-ordinating Installation Design Authority (CIDA)	Rule 3: Configuration Management / Co-ordinating Installation Design Authority (CIDA)	None
4.	Rule 4: Information Assurance	Rule 4: Vulnerability Assessment	Recast as a component of Rule 4
5.	Rule 5: Computer Network Defence (CND)	Rule 4: Vulnerability Assessment	Recast as a component of Rule 4
6.	Rule 6: Patch Management	Rule 4: Vulnerability Assessment	Recast as a component of Rule 4
7.	Rule 7: Security Accreditation	Rule 4: Vulnerability Assessment	Recast as a component of Rule 4

⁵ In accordance with the D ISS 'Requirements Coherence Process'

8.	Rule 8: Systems Safety	Rule 6: Systems Safety	None
9.	Rule 9: Performance Management	Rule 8: Network Resource Utilisation	Recast as a component of Rule 8
10.	Rule 10: Bandwidth Utilisation	Rule 8: Network Resource Utilisation	Recast as a component of Rule 8
11.	Rule 11: Packet Switched Service	Rule 9: Internet Protocol and Domain Name Service	Recast as a component of Rule 9
12.	Rule 12: Spectrum Management	Rule 10: Electromagnetic Environmental Effects	Recast as a component of Rule 10
13.	Rule 13: Messaging	Rule 11: Messaging	None
14.	Rule 14: Naming & Addressing	Rule 9: Internet Protocol and Domain Name Service	Recast as a component of Rule 9
15.	Rule 15: Directories	Rule 13: Electronic Directory Services	None
16.	Rule 16: Equipment Support	Rule 14: Equipment Support	None
17.	Rule 17: Service Continuity Management	Rule 15: Service Continuity Management	None
18.	New Rule	Rule 5	None
19.	New Rule	Rule 7	None
20.	New Rule	Rule 12	None

NETWORK JOINING RULES RISK BALANCED CASES

12. 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 consideration⁶. 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 Defence Security and Assurance Services (DSAS). The process is as follows:

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

⁶ 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 through D ISS (Head Solutions) - acting as the MOD Chief Technology Officer (CTO⁷) for CIS - 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 before submitting the case for staffing as in sub-paragraph above.
- e. If the risk balanced case is not agreed as per sub-paragraph c above, then it shall be escalated to the Departmental CIO.

ROLES AND RESPONSIBILITIES

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

Address:	DE&S D ISS Sols-C4 Architect Deputy Head Room G003 Building H4 Copenacre Site Corsham Wiltshire SN13 9NR
MOD VPN Tel:	(9)6770 0493
PSTN Tel:	030 6770 0493
MOD VPN Fax:	(9) 4382 6912
PSTN Fax	01225 846912
SMTP (Internet) e-mail:	DESISSSols-ArchGroupMail@MOD.uk

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

Address:	DE&S D ISS Sols-C4 Release & Performance Management-Service Release Authority Assistant Head Room F101 Building H4 Copenacre Site Corsham Wiltshire SN13 9NR
----------	---

⁷ The MOD CTO for CIS is the owner of technical risk for the network

MOD VPN Tel:	(9) 67700554
PSTN Tel:	0306 7700554
MOD VPN Fax:	(9)4382 6912
PSTN Fax	01225 846912
SMTP (Internet) e-mail:	DESISSSols-IntSRAGroupMail@MOD.uk

15. Comments or questions on the D ISS Customer Portal Process should be directed to:

Address:	CM Inf Man 1 Room 3 Paxcroft Bldg Rudloe Corsham Wiltshire SN13 9NR
MOD VPN Tel:	94382 6755
PSTN Tel:	01225 846755
MOD VPN Fax:	Not Available
PSTN Fax	Not Available
SMTP (Internet) e-mail:	DESISSSvcOps-CMCoord1@mod.uk

16. JSP 604 is available for download from the Defence Intranet by clicking [here](#). A copy can also be downloaded from the MoD's public intranet site at www.mod.uk.

REFERENCES

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

- a. [Information Technology Infrastructure Library \(ITIL\)](#)
- b. [The Open Group Architecture Framework \(TOGAF\)](#)
- c. [Centre for the Protection of National Infrastructure \(CPNI\) Policy and best practice: Patch Management](#)
- d. [JSP 440: The Defence Manual of Security \(Part 8: Communication and Information Systems Security\)](#)
- e. [JSP 457: Defence Manual of Interoperable Core Network Technologies](#)

- f. [JSP 480: Defence Co-ordinating Installation Design Authority \(CIDA\) Manual of regulations for installation of communication & information systems](#)
- g. [JSP 600: MOD CIS Policy and Assurance Process.](#)
- h. [JSP 602 Leaflets: Information Coherence Directions and Guidance](#)
- i. [JSP 777: NEC Handbook](#)
- j. [JSP 815: Defence Environment and Safety Management](#)
- k. [JSP 906: Design Principles for the Acquisition of Capability](#)⁸
- l. [Ministry Of Defence Architecture Framework \(MODAF\)](#)
- m. [UK MOD Deployed Technical Architecture \(DTA\)](#)
- n. [Global Information Infrastructure \(GII\) Architecture](#)
- o. [Interoperability for Communication and Information Systems](#)
- p. [DG Info/8/5/1 \(107/05\) Convergence to Defence Information Infrastructure \(DII\) Core Services, 10 Aug 05](#)
- q. [DII Application Development Guide](#)
- r. [MOD Service Oriented Architecture \(SOA\) Handbook](#)
- s. [Acquisition Operating Framework \(AOF\)](#)
- t. [DE&S Standing Instructions](#)
- u. [Service Release Handbook](#)

⁸ Currently awaiting issue

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:	<p>1. 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, policies and priorities. No minority group will detract from the benefit of the whole.</p> <p>2. Achieving maximum enterprise-wide benefit will require changes in the way we plan and manage our CIS activities. Technology alone will not bring about this change.</p> <p>3. Some organisations may have to concede their own preferences for the greater benefit of the entire enterprise.</p>
Verification & Validation Compliance:	<p>1. Reusable components shall be shared across organisation and project boundaries. Projects shall adopt the following in their solution:</p> <ul 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 services⁹ 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 overseas including Germany and Cyprus 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. National 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. <p>2. Projects shall provide evidence which demonstrates that they conform to the MOD suite of C4 Architectures and standards as described by Departmental CIO, DE&S CIO, DE&S SEIG, DE&S ISS Sols-Architect and the priorities established by the enterprise.</p>

⁹ 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.

<p>Verification & Validation Compliance (continued):</p>	<p>3. If a deviation from the above requirements is proposed then projects must clearly justify why they cannot utilise the 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 (across all DLODs) 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 as described in paragraph 12 The project is not to proceed until such an appropriate waiver is formally granted.</p> <p>Projects are required to demonstrate compliance by presenting their proposed C4 architecture to the DE&S ISS Solutions C4 Architecture team for ratification. Once ratified, the C4 Architecture team will provide an appropriate statement which shall form part of the required evidence to satisfy the Service Release Assurance requirements defined in this JSP.</p>
<p>Architecture Applicability:</p>	<p>Business Architecture Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks Technology Architecture – Security Architecture Technology Architecture – Service Management Architecture</p>
<p>Policy References:</p>	<p>JSP 906: Design Principles for the Acquisition of Capability DIN 2010DIN05-021: Defence Information Infrastructure (DII) Exemption Policy for Specialist Networks and Standalone Computers</p>
<p>Subject Matter Expertise POCs:</p>	<p>DE&S ISS Solutions-C4 Strategy Policy & Plans Deputy Head E-mail: DES ISS Sols-C4SPP Policy (MULTIUSER) DE&S D ISS Solutions-C4 Architect Deputy Head E-mail: DES ISS Sols-C4 Arch Group Mail (MULTIUSER) DE&S D ISS Programmes-Requirements Coherence Assistant Head E-mail: DES ISS Sols-Reqts Portal (MULTIUSER) DE&S D ISS Application Services Team DE&S D ISS DII Group DE&S D ISS Networks Services Team DE&S D ISS Bowman And Tactical Communication & Information Systems (BATCIS)</p>

RULE 2: LEAD BUSINESS ARCHITECT, TECHNICAL ARCHITECT, CYBER TECHNICAL ARCHITECT AND SYSTEM INTEGRATOR APPOINTMENTS

Statement:	All capability deliverers shall appoint a lead Business Architect, lead Technical Architect, lead Cyber Technical Architect and lead Systems Integrator. These Architects shall engage with the C4 Architect through the life of the capability delivery.
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> <p>The lead Cyber Technical Architect shall have responsibility for describing the logical architecture relating to the enterprise (C4 system of systems) approach on terms of Information Assurance (IA), Computer Network Defence (CND) and Service Management (SM).</p> <p>The lead Technology Architect shall have responsibility for describing the logical software and hardware capabilities (including IT infrastructure, middleware, networks, communications, processing, standards, etc) that are required to support the deployment of the business architecture.</p> <p>The System Integrator shall have responsibility for bringing together the component subsystems (including different computing systems and software applications physically or functionally) into one system and ensuring that the subsystems function together.</p>
Verification & Validation Compliance:	Evidence is to be provided that the required appointments have been made, that the personnel are suitably competent ¹⁰ and those personnel are active participants in the delivery of the capability.
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:	Defined policy is not published. Reference documentation is at: Ministry Of Defence Architecture Framework (MODAF)
Subject Matter Expertise POCs:	<p>CIO Information Strategy & Policy – Enterprise Architecture Deputy Head E-mail: CIO-ISP-EntArch DepHd – Owner of JSP 604 policy</p> <p>DE&S D ISS Solutions-C4 Architect Deputy Head E-mail: DES ISS Sols-Arch Group Mail (MULTIUSER)</p>

¹⁰ Competencies as defined in the Skills Framework For the Information Age (SFIA); roles as defined in The Open Group Architecture Framework (TOGAF)

<u>RULE 3: COORDINATING INSTALLATION DESIGN AUTHORITY (CIDA)</u>	
Statement:	<p>Before connection to the network, all capability deliverers must have an Asset Management and Configuration Management process in place.</p> <p>All CIS must provide and maintain a full documentation set and topology under configuration control through life.</p> <p>All capability providers must develop and maintain physical and environmental CIS design and installation documentation, appropriate to the required level of confidentiality, integrity and availability as defined by CIDA in JSP 480.</p>
Rationale:	Defence CIDA is mandated with the responsibility for optimising the maintenance of operational capability, flight safety and electrical security by co-ordinating changes into MOD CIS facilities and by regulating installation standards. CIDA authority applies to all sites, buildings, rooms and mobile/transportable equipment facilities but not to aircraft, ships or submarines.
Verification & Validation Compliance:	<ol style="list-style-type: none"> 1. Projects must obtain CIDA design conformance approval in accordance with JSP 480 before proceeding with installations 2. Projects must describe, demonstrate and agree with D ISS Svc Ops how they will carry out configuration management. This agreement must include details as to how they will maintain currency of the information and how the agreed set of information will be made available to the D ISS Global Operations Security Control Centre (GOSCC). 3. Projects are required to demonstrate compliance by presenting evidence of CIDA approval and agreement that configuration management proposals are to the satisfaction of D ISS as part of the required evidence to satisfy the Service Release Assurance requirements defined in this JSP.
Architecture Applicability:	<p>Technology Architecture – Infrastructure</p> <p>Technology Architecture – Networks</p> <p>Technology Architecture – Applications</p>
Policy References:	<p>JSP 480: Defence Co-ordinating Installation Design Authority (CIDA) Manual of regulations for installation of communication & information systems</p> <p>JSP 602: Leaflet 1034 'Network Mapping and Configuration Management'</p>
Subject Matter Expertise POCs:	<p>DSAS CIDA</p> <p>E-mail: DBR-DSAS-CIDA (Multiuser)</p> <p>DE&S D ISS Service Operations</p>

<u>RULE 4: VULNERABILITY ASSESSMENT</u>	
Statement:	Any capability connecting to the network must not introduce vulnerabilities to the network.
Rationale:	<p>ISS is required to maintain the integrity of the Department’s networks acting in its role as MOD Network Operating Authority. The Network Operating Authority must understand the security vulnerabilities presented by any capability connecting to the network.</p> <p>Vulnerabilities to the network can result from oversights in a number of areas of a project’s design. These may include (but may not be limited to) disclosure, loss or modification of data, compromise of component systems, propagation of malware and viruses, ineffective patching and denial of service attacks.</p>
Validation & Verification Compliance:	<p>Projects shall provide evidence that have taken all appropriate steps to ensure that they will not compromise the confidentiality, integrity or availability of the network.</p> <ol style="list-style-type: none"> 1. Projects shall provide evidence that an independent information assurance computer security audit has been conducted and that the recommendations will be risk managed in agreement with the Accreditor(s) and Network Operating Authority. 2. Projects shall provide evidence that they have a relevant system security accreditation from their DSAS appointed security accreditor. 3. Projects shall provide evidence that they will not compromise the Network Operating Authority’s (NOA) mandate to conduct OP METRIC. This evidence shall clearly demonstrate that the project has engaged with the D ISS C4 Security Architects and D ISS Svc Ops team and gained approval from those teams that planned capability will not compromise ISS’s remit to protect Departmental CIS systems. Broadly, projects shall permit the NOA to conduct real time network situational awareness of their systems. This will include the use of passive and active methods such as deployed software clients (eg the Establish the Baseline (EtB) client Eracent), network scanning (eg the enhanced CND capability) and the deployment of intrusion detection/prevention (IDS/IPS) equipment. In addition, projects must make provision to provide NOA with network configuration data on a regular basis and additionally during a CND incident. 4. Projects shall engage with the ‘Establish the Baseline’ (EtB) project to ensure that there are no interoperability issues with the Eracent client. The client must be installed on any hardware that is capable of hosting it and all software (including patches, service packs, upgrades etc) must be fingerprinted such that they are recognised by Eracent. Furthermore, projects must demonstrate that they have a working process that ensures that EtB are notified when a capability is disposed of (this includes software, firmware or hardware). 5. All systems that have software or firmware components shall have an approved patch management policy and established set of supporting procedures. The policy/procedures must include a DSAS approved security vulnerability patching method. All patches and 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. 6. All systems/projects must include a coherent through life management plan for software, firmware and hardware (SFH). The plan must show when and how SFH will be updated or replaced in accordance with vendor product lifecycles. This means that only SFH that is fully vendor supported will be permitted to operate on MoDs networks. 7. Evidence that the above requirements have been met shall be provided to the Service Release Authority to demonstrate compliance with this JSP.

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>JSP 440: The Defence Manual of Security (Part 8: Communication and Information Systems Security)</p> <p>JSP 480: Manual of Regulations for Installation of Communication and Information Systems</p> <p>Centre for the Protection of National Infrastructure (CPNI) Policy and Best Practice: Patch Management</p> <p>Best Practice: Information Technology Infrastructure Library (ITIL) V3</p>
Subject Matter Expertise POCs:	<p>DE&S D ISS Solutions-C4 Strategy Policy & Plans-Policy 1</p> <p>E-mail: DES ISS Sols-C4SPP Policy (MULTIUSER)</p> <p>DE&S D ISS Service Operations-Operations DIO-SA Hd</p> <p>E-mail: DES ISS SvcOps-OPS DIO Front Door</p> <p>DSAS-DDAcc</p> <p>E-mail: DSSO-DDAcc (Archer, Tammy Mrs)</p> <p>DE&S D ISS Network Services Team (ECND Project)</p> <p>Email: TBA</p> <p>DE&S D ISS Establish the Baseline Team (ECND Project)</p> <p>Email: TBA</p>

<u>RULE 5: QUALITY OF SERVICE</u>	
Statement:	ISS has a responsibility to deliver and manage the Department’s funded CIS needs in an efficient and effective manner ensuring that priority services meet their agreed service levels. One such mechanism is through the definition of a ‘Quality of Service’ for IP based services. Projects are to ensure that any IP based capability they introduce is able to support QoS through the use of Differentiated Service Code Point (DCSP).
Rationale:	Quality of Service is the technical ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. This may include for example a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed. Quality of service guarantees are important where network the network may be reaching capacity or it is a limited resource.
Validation & Verification Compliance:	Projects shall submit a formal declaration that they comply with MOD policy and have sought guidance from the C4 Architects.
Architecture Applicability:	Business Architecture Information Systems Architecture – Data Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks
Policy References:	Currently being drafted
Subject Matter Expertise POCs:	DE&S D ISS Solutions-C4 Architect Deputy Head E-mail: DES ISS Sols-C4 Arch Group Mail (MULTIUSER)

<u>RULE 6: SYSTEMS SAFETY</u>	
Statement:	Safety Cases are to be developed for all CIS applications, infrastructure and networks. A Safety Case must be suitable and sufficient for the particular project or programme. The effort involved in preparing and maintaining the Safety Case shall be commensurate with the level of safety risk. Safety Cases shall be produced by individuals who are suitably qualified and experienced to do so. The Safety Case shall be reviewed at appropriate times throughout the lifetime of the project or programme. These intervals and/or criteria for review shall be clearly stated.

Rationale:	<p>Ensure that, where necessary, a suitable and sufficient safety case has been produced in order to meet legal requirements.</p> <p>Safety Cases contain evidence that the delivered product, equipment or service is safe. Failure to comply with legislation, or follow MoD policy and instructions could lead to inadequate safety cases and hence delivery of unsafe products, equipment or services, with the associated risk of censure or prosecution.</p>
Verification & Validation Compliance:	Projects are to comply with the extant guidance in the AOF and provide the Service Release Authority with evidence of an approved Safety Case or Statement (as appropriate) for the capability being released.
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>JSP 815: Defence Environment and Safety Management</p> <p>DE&S Standing Instructions SI 14 – Acquisition Safety & Environment Mgmt</p> <p>Acquisition Safety & Environmental Management System (ASEMS)</p>
Subject Matter Expertise POCs:	<p>DE&S D ISS Programmes-Acquisition Safety and Environment Team</p> <p>E-mail: DES ISS Progs-Acq Safety 2</p> <p>Tel: 0306 7700686</p>

<u>RULE 7: INTEGRATED NETWORK MANAGEMENT</u>	
Statement:	<p>All projects must ensure that they comply with technical performance management requirements as defined down by the Network Operating Authority (this is to include those capabilities that constitute the network). This applies to new capabilities as well as upgrades and changes.</p> <p>Specifically all projects must provide correlated service affecting events using the SNMP protocol with the following fields populated (as a minimum): Service; Summary; Alert Group; Event Type; Cause Type; Severity & Last Occurrence.</p>
Rationale:	<p>The Department's IS systems and infrastructures are in the main large, dynamic and diverse creating a high degree of complexity. To deliver effective IS services there is a requirement to be able to anticipate the impact of CIS changes, proactively monitor performance, accelerate problem resolution, control network configurations and changes and keep capital and operating costs down.</p> <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>
Verification & Validation Compliance:	Projects shall demonstrate, through appropriate testing on a representative environment, agreed with the DE&S ISS Solutions Test and Evaluation Team, that they are able to produce 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:	Technical Performance Management Architecture – To be developed
Subject Matter Expertise POCs:	<p>DE&S D ISS Service Operations</p> <p>DE&S D ISS Integration Continual Service Improvement</p>

<u>RULE 8: NETWORK RESOURCE UTILISATION</u>	
Statement:	All new or changed CIS projects will have an affect on CIS resources. Projects must quantify the extent of that affect and demonstrate that appropriate network resources are available to support the capability (in accordance with the capability's defined ConUse). The capacity and availability of existing CIS capabilities shall be maintained following implementation.
Rationale:	The Department's IS systems and infrastructures are in the main large, dynamic and diverse creating a high degree of complexity. To deliver effective IS services there is a need for capabilities to quantify the network resources they will consume.

<p>Implications:</p>	<p>Any application (or other capability) that plans to operate over the GII must demonstrate that Network resources and behaviour are sufficient to support the solution and do not have a detrimental impact on other services ie they are a 'good neighbour'.</p> <p>Projects shall ensure and provide evidence that:</p> <ul style="list-style-type: none"> • The network resource requirements are appropriately defined and quantified. • Any application is designed with the network constraints as a primary consideration. This shall include, but is not limited to, latency, capacity and quality of service. • Appropriate testing on a representative environment, agreed with the DE&S ISS Solutions Test and Evaluation Team, is undertaken to demonstrate acceptable behaviour on the network. • Testing is to be conducted in a simulated network and physical network environment, both representative of the live network environment. • Post go live, an appropriate evaluation is undertaken to demonstrate the actual behaviour on the network. This must also show a comparison with the pre-go live quantification. <p>Projects are strongly encouraged to conduct an 'Application Characterisation' to assist in the generation of this evidence.</p>
<p>Architecture Applicability:</p>	<p>Business Architecture Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks</p>
<p>Verification & Validation Compliance:</p>	<p>Projects are to present their interpreted evidence to the Service Release Authority. This evidence, drawn from testing in a representative test environment, shall clearly demonstrate the network resources that the capability will consume and the behaviour it will exhibit.</p> <p><u>Applications:</u></p> <ul style="list-style-type: none"> • Production of network traffic profiles relevant to a stated ConUse. Profiles must be supported by tests conducted in a representative live environment which reflects the subject network constraints (e.g. bandwidth, latency, security). • Confirmation that the network resource required to support the traffic profiles is available. • Demonstration that the application performs in the expected manner across a representative live network. (For projects to be deployed on Op HERRICK this testing must be conducted at the LSRC where possible). These tests should include as a minimum: <ul style="list-style-type: none"> ○ Replication of the scheduled Site Acceptance Tests (SATs) ○ Replication of any User Acceptance Trials (UATs) that could be impacted by the constraints of the live network ○ Demonstration of satisfactory operation of all information interfaces with other systems. ○ Affects on the application of network bandwidth throttling. ○ Affects on the application of network latency. ○ Affects on the application of link failure – eg. Short glitches,

	<p style="text-align: center;">prolonged outages etc.</p> <p><u>Network Projects:</u></p> <p>The project must demonstrate that the new or modified network component can integrate with the existing network and continues to support existing infrastructure and associated applications. Demonstration testing shall be performed in a representative live environment and will include as a minimum:</p> <ul style="list-style-type: none"> • Replication of the Site Acceptance Tests (SATs) • Correct operation of Physical Interfaces • Correct operation of Electrical Interfaces • Successful end-to-end transfer of project pre-prepared test patterns and information scripts, representative of current network usage, e.g. e-mail, web apps, client-server, server-server, voice services. <p><u>Infrastructure Projects:</u></p> <p>The project shall demonstrate that the new or modified infrastructure element integrates with the existing infrastructure and onto the chosen network. It must also continue to support the existing application services.</p>
Policy References:	<p>JSP 602: 1030 – Wide Area Bandwidth</p> <p>MODAF View SV-7: Resource Performance Parameter</p>
Subject Matter Expertise POCs:	<p>DE&S D ISS Solutions-Integration Service Release Authority</p> <p>E-mail: DES ISS Sols-Int SRA GroupMail (MULTIUSER)</p>

<u>RULE 9: INTERNET PROTOCOL (IP) AND DOMAIN NAME SYSTEM (DNS)</u>	
Statement:	<p>All systems must be IPv4 based both internally and at the gateways. IPv4 addressing and routing must comply with current Defence policy.</p> <p>All equipment procured must be <u>capable</u> of supporting IPv6 either now or as a result of an identified manufacturer’s roadmap for providing IPv6 capability. However, IPv6 must not be enabled on the network until its use has been sanctioned by Defence policy.</p> <p>DNS must be operated in accordance with current Defence policy, including concept of operation, configuration and the use of official MOD namespace hierarchies.</p>
Rationale:	<p>Standardisation of network communication protocols, as represented at Layer 3 of the OSI Reference Model, allows for compatibility between any network-connected device. IPv4 and IPv6 are the de facto standard Layer 3 network protocols.</p> <p>A future migration to IPv6 will require careful planning and Defence-wide coordination in order to maintain interoperability and security.</p> <p>DNS is the de facto standard for providing an abstract name-based method for interaction with the IP addressing space.</p>
Validation & Verification Compliance:	<p>Projects shall submit a formal declaration that they comply with MOD policy and have sought guidance from the SME.</p>

Architecture Applicability:	Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks
Policy References:	JSP 457 Volume 1 – IP and DNS DIN 2006DIN04-096 – Interim Defence Policy on IPv6
Subject Matter Expertise POCs:	DE&S D ISS Solutions-Architect Deputy Head E-mail: DES ISS Sols-Arch Group Mail (MULTIUSER)

RULE 10: ELECTROMAGNETIC ENVIRONMENTAL EFFECTS

Statement:	The project team shall demonstrate that the capability shall not cause unacceptable levels of electromagnetic interference to existing systems. Furthermore, it shall also be demonstrated that the appropriate frequency allocations have been applied for and granted.
Rationale:	To maximise the effect of capabilities it is crucial that measures are taken to protect all classified non communication electromagnetic emission from detection by hostile forces or organisations. Radio spectrum is a scarce resource and must be managed in an efficient and effective manner. To ensure that we continue to interoperate with our allies and NATO partners it is crucial that there is a standardised approach to spectrum usage.
Verification & Validation Compliance:	The Defence E3A organisation must approve any system that utilises electromagnetic transmissions. Projects shall submit evidence to the Service Release Authority to demonstrate that they have sought guidance from the SME, that they comply with MOD policy and they have secured the appropriate spectrum they require.
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

RULE 11: MESSAGING

Statement:	Low and medium grade messaging systems must utilise SMTP as their primary transport protocol. Legacy systems must have a transition plan demonstrating how and when they plan to migrate from X400 to SMTP. High grade messaging systems must comply with applicable extant policies.
------------	--

Rationale:	There is an aspiration for MOD to adopt SMTP as opposed to X400 for its primary (or sole) protocol for low/medium grade e-mail messaging. Benefits of Defence-wide use of SMTP include increased interoperability, reduced system complexity, wider vendor/product choice and alignment with de facto international standards and best current practice.
Verification & Validation Compliance:	Projects shall submit evidence to the Service Release Authority to demonstrate that they have sought guidance from the SME and that they comply with MOD policy.
Architecture Applicability:	Information Systems Architecture – Data Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks
Policy References:	Defence Messaging Policy JSP 457
Subject Matter Expertise POCs:	CIO-J6 Policy CIO-J6-Pol2 DE&S D ISS Solutions-Architect Deputy Head DES ISS Sols-C4 TechArch 2 DE&S D ISS DII Engineering Management

<u>RULE 12: CODES OF CONNECTION</u>	
Statement:	Any project that has a requirement to interconnect with other extant CIS systems shall conform to that system's Code of Connection policy. Any such connection shall not introduce an unacceptable risk to the current network.
Rationale:	Adherence to agreed Codes of Connection (CoCo's) maximise the ability for Departmental systems to seamlessly interconnect. This allows systems/services to exchange data and information in a managed and effective manner, within an acceptable risk envelope.
Verification & Validation Compliance:	Projects shall provide evidence that they have complied with the appropriate Codes of Connection ('CoCo's) for any CIS system they interface with. This should include any onward connection to non-Departmental systems.
Architecture Applicability:	Information Systems Architecture – Data Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks
Policy References:	JSP 440 Part 8, Section 5, Chapters 2 & 9 JSP 440 Part 8, Section 5, Chapter 4 and Chapter 4, Annex E

Subject Matter Expertise POCs:	<p>DE&S D ISS Solutions-C4 Architect Deputy Head E-mail: DES ISS Sols-C4 Arch Group Mail (MULTIUSER)</p> <p>DE&S D ISS Programmes-Requirements Coherence Assistant Head E-mail: DES ISS Sols-Reqts Portal (MULTIUSER)</p> <p>DE&S D ISS Application Services Team</p> <p>DE&S D ISS DII Group</p> <p>DE&S D ISS Networks Services Team</p> <p>DE&S D ISS Bowman And Tactical Communication & Information Systems (BATCIS)</p>
--------------------------------	---

<u>RULE 13: ELECTRONIC DIRECTORY SERVICES</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:	An essential enabler of electronic communication is an effective pan-Defence directory service that adheres to common protocols, standards and formats. This requirement is satisfied by the development and maintenance of a Defence wide electronic directory providing ready access to all significant contact information such as messaging, electronic, postal and PKI related attributes.
Verification & Validation Compliance:	Projects shall submit a formal declaration that they comply with MOD policy and have sought, and applied, guidance from the Directories Steering Board.
Architecture Applicability:	<p>Business Architecture</p> <p>Information Systems Architecture – Data</p> <p>Information Systems Architecture – Applications</p> <p>Technology Architecture – Infrastructure</p>
Policy References:	<p>JSP 602:1009</p> <p>JSP 457: Volume 4</p>
Subject Matter Expertise POCs:	<p>DE&S D ISS Solutions-Architect Deputy Head</p> <p>E-mail: DES ISS Sols-Arch Group Mail (MULTIUSER)</p> <p>DE&S D ISS DII Engineering Management</p>

<u>RULE 14: EQUIPMENT SUPPORT</u>	
Statement:	Detailed Equipment Support and Service Support policy and procedures shall be in place. These plans shall include clear detail of the through life requirement (including disposal or termination) for CIS services and support.

Rationale:	Any deliverer of capability must consider from the earliest stages of the project lifecycle how the equipment or capability will be supported, maintained and sustained through life. Every reasonable effort must be taken to ensure that the equipment's CIS support requirements do not place undue and unfunded burden on the CIS community.
Verification & Validation Compliance:	Projects shall demonstrate that they have appropriate equipment support arrangements in place and that they have complied with the requirements with the AOF and Support Solutions Envelope. Evidence is also required to demonstrate that secured funding is in place.
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 (AOF) JSP 899 – Logistics Process Roles and Responsibilities JSP 503 – Business Continuity Management Support Solutions Envelope
Subject Matter Expertise POCs:	DE&S D ISS Service Operations

<u>RULE 15: SERVICE CONTINUITY MANAGEMENT</u>	
Statement:	Projects shall demonstrate how services will be maintained in the event of a major incident. The goal of Service Continuity Management is to support the overall business continuity management process by ensuring that the required IT Technology and service facilities (including computer systems, networks, applications, data repositories, telecoms, environment technical support and service desk) can be resumed within required and agreed business timescales.
Rationale:	As technology is a core component of most business processes, continued or high availability of IT is crucial to the survival of the business as a whole. This is achieved by introducing risk reduction measures and recovery options.
Verification & Validation Compliance:	Projects must demonstrate how their system will be maintained in the event of a major incident and how they will continue to deliver their minimum service level agreements. They must demonstrate how the failure and subsequent recovery procedures will impact on the network. These must be tested on a representative test and reference environment and be acceptable to the Network operating Authority.

Architecture Applicability:	Business Architecture Information Systems Architecture – Data Information Systems Architecture – Applications Technology Architecture – Infrastructure Technology Architecture – Networks
Policy References:	Best Practice: ITIL v3
Subject Matter Expertise POCs:	DE&S D ISS Service Operations

PROPOSED NETWORK JOINING RULES

JSP 604 will evolve with time. This section provides the reader with an indication of rules that are being considered and developed for inclusion in future versions of the document.

1. Network Configuration Management
2. Change of the DII/F Operating System to Windows 7