JSP 602 Instruction	9999	**Applicability**	Applications, Data/Information, Infrastructure, Integration, Legislation, Network/Communications, Security
Configuration Identity	Version: 01.02 Amended: 2009-03-02 Reviewed: 2006-06-20	**Epoch Applicability**	2005 - 2009

JSP 602: 9999 - How to Read a JSP602 Leaflet

Outline

Description: A brief description of the policy covered in the policy leaflet.
Reasons for Implementation: A brief statement of why the policy should be implemented.

Issues: Any issues pertinent to this policy and its implementation that need to be exposed.

Guidance: Any guidance that is associated with this policy including its conformance with both the e-GIF (i.e. national policy with which MOD must comply) and the NC3TA (i.e. international policy that MOD has ratified and with which it must comply), plus any deviations from them.

A statement of any overall mandatory policy where applicable.

Policy

Strategic

9999.01: Policy Category Title

9999.01.01 Policy statement text - a statement of policy that includes its applicability and, where appropriate, caveats the list of standards that follow it. The statement is prefixed by a unique reference number.

> **9999.01.01.01** standards to be used (including reference); where several standards are required,
> each one is shown as a separate list item.
>
> *Comment:* The standards mandated for the policy are shown as a bulleted list. In some instances the bullets may identify the mandatory properties/features of a system/project.

Rationale for the policy statement can be included where appropriate.

Comment: Comment text - where necessary, comments can be used to support the policy statement.

9999.01.02 Policy statement text **-** a statement of policy that includes its applicability and, where appropriate, caveats the policy sub-statement that follows it. The statement is prefixed by a unique reference number.

> **9999.01.02.01** A policy sub-statement **-** this is a sub-division of the policy statement and will generally be used to break the policy down into a set of simpler statements **-** it is not a standard.
> It is prefixed with a unique reference number.
>
> *Rationale can be associated with a policy sub-statement*
>
> *Comment:* Comments can be associated with a policy sub-statement.
>
> > **9999.01.02.01.01** Standards **-** where a policy sub-statement demands the implementation of one or more standards, these can be added. They are prefixed by a unique reference number.
> >
> > *Rationale can be associated with the standards.*
> >
> > Comment: Comments can be associated with the standards.

Rationale for including this policy category can be included.

Comment: Policy within a leaflet is divided into a series of policy categories, each having a title prefixed by a unique reference number. Categories will contain one or more policy statements. Within the policy table all systems/projects must look at each Policy Category and the policies within them to see if/how they apply to them. They must also be aware that a system/project could be delivering into more than one of the domains (strategic, deployed etc) and hence must consider the applicability of the policy within each domain as necessary.

9999.02: Definition of Strategic Domain

9999.02.01 The Strategic Domain as used within the 602 policy leaflets is defined as follows:

Strategic (continued)

9999.02.02 A primarily office-based domain with high capacity, high availability local infrastructure (LAN) and high capacity, high availability external connections (WAN). User devices (workstations, software etc.) are highly capable (in terms of processing power, memory capacity, interfaces, screen size and resolution etc.) being standard commercial items. Users and equipment operate in a largely benign environment with few constraints (see definition of constraints below). Security requirements can range from minimal to severe (UC to TS). Replacement/upgrade of equipment is generally simple to achieve and low in cost. Examples of this include MOD offices and defence sites within the UK and overseas garrisons such as Cyprus, Gibraltar and the Falklands; also included will be ships/submarines whilst 'alongside' and connected directly to the RLI/SLI and home workers connected via broadband to the fixed infrastructure.

9999.03: Definition of constraints

9999.03.01 These are constraints imposed by the operating environment and include such factors as temperature, humidity, pressure, vibration, shock, EMC, EMP, particle contamination, power supplies (quality and availability) and physical size.

Deployed

9999.04: Policy Category Title

9999.04.01 Policy statement text.

> **9999.04.01.01** standards to be used (including reference).
>
> *Rationale for the standard where appropriate.*
>
> *Comment:* Comment text relating to the policy standard.

Rationale for the policy where appropriate.

Comment: Comment text relating to the policy statement.

Rationale for the policy category where appropriate.

Comment: Comment text relating to the policy category.

9999.05: Definition of Deployed Domain

9999.05.01 The Deployed Domain as used within the 602 policy leaflets is defined as follows:

9999.05.02 A primarily temporary or semi-permanent domain with high capacity, high availability local infrastructure (LAN) and medium or low capacity, medium or low availability external connections (WAN). User devices (workstations, software etc.) are highly capable (in terms of processing power, memory capacity, interfaces, screen size and resolution etc.) being standard commercial items with some ruggedisation. Users and equipment operate in a non-benign environment that imposes significant environmental constraints. Security requirements can range from significant to severe (R to TS). Replacement/upgrade of equipment is generally simple to achieve and low in cost before deployment but harder and higher in cost during a deployment. Examples of this include major deployed headquarters such as the JFHQ (including JFHQ afloat), Divisional HQ, Formation-level HQ, major warships (frigates and above) whilst at sea and forward airfields.

Tactical

9999.06: Policy Category Title

9999.06.01 Policy statement text.

9999.06.01.01 standards to be used (including reference).

Rationale for the policy and or standards where appropriate.

Comment: Comment text.

9999.07: Definition of Tactical Domain

9999.07.01 The Tactical Domain as used within the 602 policy leaflets is defined as follows:

9999.07.02 A primarily temporary or mobile domain with limited local infrastructure (LAN) and medium to very low capacity , medium to low availability external connections (WAN). User devices (workstations, software etc.) have limited capability (in terms of processing power, memory capacity, interfaces, screen size and resolution etc.) being largely bespoke items with considerable ruggedisation. Users and equipment operate in an often hostile environment that imposes severe environmental constraints. Security requirements can range from significant to severe (R to TS). Replacement/upgrade of equipment is generally hard to achieve and is consequently high in cost. Examples of this include deployed headquarters (with no step-up function) such as Battlegroup HQ, military vehicles, minor warships and submarines (at sea) and aircraft.

Remote

9999.07: Policy Category Title

9999.07.01 Policy statement text.

9999.07.01.01 standards to be used (including reference).

Rationale for the policy where appropriate.

Comment: Comment text.

9999.08: Definition of Remote Domain

9999.08.01 The Remote Domain as used within the 602 policy leaflets is defined as follows:

9999.08.02 A domain covering primarily (though not exclusively) mobile users with little or no local infrastructure and low capacity, low availability external connections (WAN) that can be maintained on the move. User devices (mobile phones, PDAs, software etc.) have limited capability (in terms of processing power, memory capacity, interfaces, screen size and resolution etc.) being largely small form-factor standard commercial items with little or no ruggedisation. Users and equipment operate in typically benign environment that imposes few environmental constraints. Security requirements can range from minimal to significant (UC to R). Replacement/upgrade of equipment is generally simple to achieve and low in cost. Examples of this include mobile users connecting to the infrastructure through a dial-up connection (mobile phone or land line) and home workers using a narrow band connection.

Responsibility for Implementing the Policy

Identifies which types of system/project are responsible for implementing the policy contained within the leaflet.

Procedure

Includes, where possible, procedures to clearly identify how the mandated policy and standards will be implemented, making reference to documents where required. Where a particular authority and/or IPT is the principal provider of a service or provider of technical support, then this will be identified here together with relevant contact details.

Relevant Links

All external links are listed here. These will include links to other JSP602 leaflets, other policy document such as JSPs and Def-Stans and relevant AMS guidance.

A glossary of terms and abbreviations used within this document is available here.

Compliance

Stage	Compliance Requirements
Initial Gate/DP1	Includes evidence pertaining to Initial Gate (in CADMID terms) or DP1/Authorising Project Initiation (in PRINCE 2 terms) that must be presented by projects to demonstrate their compliance with the policy. At this stage in a project the requirements are typically implementation/technology independent (i.e. as defined within the URD). Compliance with technical policy will therefore be general in nature but ensuring that proper consideration is given at later project stages.
Main Gate/DP2	Includes evidence pertaining to Main Gate (in CADMID terms) or DP2/Authorising A Project (in PRINCE 2 terms) that must be presented by projects to demonstrate their compliance with the policy. At this stage in a project the requirements are implementation/ technology specific (i.e. as defined within the SRD) but implementation details are unknown. Compliance with technical policy will therefore be typically stated in terms of the policy categories that apply and the standards to be used. This information will be typically captured within MODAF technical standards views.
Release Authority/DP5	Includes evidence pertaining to DCSA RACA provided as part of System Acceptance (in CADMID terms) or DP5/Confirming Project Closure (in PRINCE 2 terms) that must be presented by projects to demonstrate their compliance with the policy. Evidence will typically cover conformance with standards or prescribed processes. Standards conformance evidence can be gathered from a range of sources as appropriate such as: 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 appropriate Defence Test and Reference Facilities.