JSP 602 Instruction	1005	**Applicability**	Applications, Infrastructure
Configuration Identity	Version: 01.03 Amended: 2009-18-01 Reviewed: 2009-18-01	**Epoch Applicability**	2008 - 2011

JSP 602: 1005 - Collaboration Services

Outline

Description: Collaboration Services describes the protocols and standards that are used to enable the collaborative working of many users distributed across the GII. They fall into two categories: real-time collaboration services, where participants interact concurrently as if they were co-located (e.g. whiteboarding); and non real-time, where participants submit questions or comments and receive a response some time later (e.g. news groups).

Reasons for Implementation: The Defence Information Strategy requires collaborative and flexible working patterns in order to meet rapidly changing requirements. Collaborative working enables dispersed users to carry out business processes, work on a single application and/or use data from a single source in order to jointly pursue business benefits. A collaborative working environment for business and operational functions is essential to facilitate the communication and transfer of thoughts and ideas between collaborative partners. Standardisation is necessary to ensure that collaboration services provided and hosted on the GII will interoperate effectively.

Issues: Some real-time collaboration services, such as video conferencing, require good QoS to be provided by the network, specifically low error rates and low latency. Their use in low bandwidth environments must be carefully controlled if permitted at all.

Collaboration service protocols can present security risks; hence their use across security domains must be in line with security policy.

For collaborative working to be effective, factors such as data management and utilisation of appropriate information and communication infrastructures are vital considerations. It is also important to ensure that both the applications and data are interoperable.

Guidance: Collaborative working can take place at a number of levels. At the simplest level, Collaborative Working is different personnel at a single site each having access to a shared work area. More complex examples of Collaborative Working are the creation and utilisation of shared working environments that span functional, organisation and international borders. Collaborative working is fundamentally about business processes, whereas Shared Working or Shared Data Environments are the underpinning IT infrastructure and toolsets to enable collaborative working.

Guidance on the commercial policy on collaborative working can be found in the Guidelines for Industry, Section 15 (issue 2) - Shared Data Environments, which can be found on the Commercial Manager's Toolkit on the AMS and on the DG Commercial Web Page. The guidance describes the use of model contract conditions and an Electronic Information Sharing Agreement to enable collaborative working between MOD and its suppliers. The guidance and supporting documentation has been negotiated with the Confederation of British Industry and

other trade associations and its use is therefore highly recommended. Any enquiries on the matter should be addressed to PDC Commercial Policy on Ensleigh (9355) 67260.

Any MOD projects that contain interaction with dispersed organisations should consider a requirement for collaborative working, including shared data environments, integrated applications or common business processes. Shared working areas should have a clearly defined Senior Responsible Owner along with clearly defined processes and documentation.

This leaflet is consistent with the e-GIF with the following exception:

- the e-GIF does not address real-time collaborative services;
- the e-GIF does not address server-server interactions.

This policy is consistent with the NC3TA.

Policy

Real-time collaboration services:

Strategic

1005.01: Whiteboarding

1005.01.01 All systems and/or projects providing whiteboarding services shall do so using the following standards:

1005.01.01.01 ITU-T T.126 - Multipoint Still Image and Annotation Conferencing Protocol Specification

A de facto standard with extensive product support that defines the protocol used to provide interoperability with graphics data in applications such as whiteboarding, annotated image exchange, screen sharing and remote applications control

1005.01.02 All systems and/or projects implementing the streaming protocols listed above shall ensure that they do not cross over security domain boundaries.

Comment: Server-server model - Current server products are not interoperable due to call setup, compression and non-standard protocols.

1005.02: Video Conferencing

1005.02.01 All systems and/or projects requiring video conferencing services shall do so using the following standards:

1005.02.01.01 ITU-T H.323:2003 - Packet-based Multimedia Comms System

A de facto standard with extensive product support for interoperability in audio, video and data transmissions as well as internet and VoIP that promotes consistency.

Comment: These packet-based video conferencing standards support 1-to-1, 1-to-many and many-to-many conferences.

1005.02.01.02 ITU-T T.120:2002 - Data Protocols for Multimedia Conferencing

A de facto standard with extensive product support that enables real-time multi-point data communications including desktop data conferencing and multi-user applications.

Comment: There are a number of risks associated with server-to-server interactions. Loss of a master server will disrupt a WAN session until new master is declared and configured in the server constellation. Replication of Data Repository may be necessary across servers - tendency is for products to create a single Data Repository. For voice and video - choice of CODEC must reflect bearer capability. In addition to providing a VTC Service at the Top Secret security level to UK Defence users and Defence Industry partners the DFTS Managed VTC Service has connectivity at Secret level to both the US and NATO VTC Services.

1005.03: Server-to-server interactions

1005.03.01 All systems and/or projects providing any of the real-time collaboration services defined above shall ensure that only server-to-server interactions are permitted across the WAN.

Strategic (continued)

Comment: Enforcing server-to-server interactions only across a WAN provides a number of benefits. Access control to conferences and data repositories is supported (by making users log-in to a conference and letting others know who is in the conference). Security is enhanced by maintaining strict control over port and IP address assignments for streaming protocols. Bandwidth and CODEC allocations can be managed on a per-conference basis. Individual Data Repositories can be associated with each conference and the structure of meeting space can be managed as multiple virtual meeting rooms.

Deployed

As for Strategic domain.

Tactical

1005.04: Video Conferencing

1005.04.01 All systems and/or projects requiring video conferencing services shall do so using the following standards:

1005.04.01.01 ITU-T H.323:2003 - Packet-based Multimedia Comms System

1005.04.01.02 ITU-T T.120:2002 - Data Protocols for Multimedia Conferencing

Bandwidth and QoS limitations will rule out 1:many and many:many collaborative sessions.

Comment: H.323/T.120 are streaming protocols and therefore are a security issue, hence can only exist within a single security domain. For voice and video - choice of CODEC must reflect bearer capability.

Remote

As for Strategic domain.

Comment: A remote client will be treated as if it were any other node on a network; hence it can participate in collaborative sessions in the same way as any local client.

Policy

Non real-time collaboration services:

Strategic

1005.05: Mailing Lists

1005.05.01 All systems and/or projects providing formal and interpersonal messaging services shall conform to the policy contained within JSP602: 1016 Messaging Services.

The handling of mailing lists is part of the messaging standards and are widely supported. They are simple to implement and maintain.

Comment: Mailing lists are a common method of distributing information to collaborating groups. As a method of distribution it does, however, exhibit scalability problems that can lead to network and system overload due to messages being sent many times.

1005.06: E-Business

1005.06.01 All MOD sectors and departments requiring the provision of new e-Business services shall contact their appropriate DCSA CRM.

1005.06.02 The policy for the use of certificates to secure e-Business transactions is contained within JSP602: 1004 - Certificate services.

1005.07: Portals/Web Sites

1005.07.01 All systems and/or projects providing Web Portals and/or Web Sites shall support the following standards for information publishing:

1005.07.01.01 HTML, Version 4.0.1, Reference Specification, W3C REC-html401-19991224:1999 (Dynamic HTML)

1005.07.01.02 XHTML, version 1, W3C RECxhtml1-20020801:2002

1005.07.01.03 XML version 1.0 (Second Edition), W3C REC-xml-20001006:2000 - (see JSP602: 1031 XML)

These are the de facto standards for advertising and disseminating information and services that support specific communities of interest.

1005.07.02 All systems and/or projects providing Web Portals and/or Web Sites shall support the following standards for information access:

1005.07.02.01 HTML, Version 4.0.1, Reference Specification, W3C REC-html401-19991224:1999 (Dynamic HTML)

1005.07.02.02 XHTML, version 1, W3C RECxhtml1-20020801:2002

1005.07.02.03 WML version 2, WAP Forum WAP-238-WML-20010911-a:2001 - for WAP phones

Strategic (continued)

1005.07.02.04 HTTP v1.1 (RFC 2616), URL (RFC 1738), URI (RFC 2396) - Hypertext transfer Service

These are the de facto standards for accessing web-delivered information and services.

1005.07.03 All systems and/or projects providing Web Portals and/or Web Sites shall provide support for low function browsers.

Comment: Mobile access to the MOD information infrastructure is becoming increasingly necessary from devices such as PDAs and Mobile Phones (that have limited browsing capabilities) and where full web page content cannot be supported. To this end a range of low function browsers exist with limited rendering and user interaction capabilities.

1005.07.04 All systems and/or projects providing Web Portals and/or Web Sites shall conform to the MOD policy on meta data declaration contained within JSP602: 1008 - Defence Data.

1005.08: News Groups

1005.08.01 All systems and/or projects requiring news group functionality shall use the following standard:

1005.08.01.01 NNTP (RFC 977) - Bulletin board service

The de facto standard for News Services. This approach is bandwidth friendly as information only travels once across the WAN.

1005.08.02 News Servers shall, where possible be located geographically close to the communities they serve (i.e. News Server topology should reflect network topology)

Client access to News Servers should remain within the local area network where at all possible.

Comment: This is a subscription service whereby users sign up to particular News Groups held within a local News Server. Access to News Servers can be controlled. However, access to individual News Groups within a server cannot be controlled (except by use of encryption).

Deployed

As for Strategic domain.

Tactical

1005.09: Data Sharing

1005.09.01 All systems and/or projects providing collaboration services shall use the following standards:

1005.09.01.01 JC3IEDM, NATO STANAG 5525

The common data interchange specification of NATO.

Remote
As for Strategic domain. *Comment:* A remote client will be treated as if it were any other node on a network; hence it can participate in collaborative sessions in the same way as any local client.

Responsibility for Implementing the Policy

Implementation of this policy shall be the responsibility of all IPTs (and their suppliers) that provide collaboration services across the GII.

Procedure

In the strategic environment VTC is provided as a managed service by DFN IPT. This service shall be used unless there is a justifiable technical or financial reason for an alternative strategy. If this route is being considered, technical advice must be sought from the Through Life Manager of VTC services, DCSA DFN Mobility 2b:(COP-H4-B210, 3474COR, Tel: 01225 813474).

DECS is a corporate enabler for collaborative working between the MOD and its suppliers (trading partners). It also provides the ability to enable IPTs and their main suppliers to share project and product data. The DECS Core Shared Working Environment is the default for information sharing within Collaborative Working Environments for the DLO.

Information on the use of DECS can be obtained from the DCSA DCBA IPT on Corsham (94382) 3768 or 3155.

For information on the user aspects of Collaborative Working DG Information is the lead organisation. Projects should contact AD Information Management, Minerva House on (96381) 5272

Relevant Links

JSP602: 1007 – Database Services

JSP602: 1008 - Defence Data

JSP602: 1016 - Messaging Services

JSP602: 1004 - Certificate Services

Guidelines for Industry, Section 15 (issue 2) - Shared Data Environments can be found here. (http://www.ams.mod.uk/ams/content/docs/toolkit/buttons/modind/gfi15.htm)

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

Details of HTML, XHTML and XML can be found on the W3C web site here.
(http://www.w3.org/)

Details of WML can be found on the WAP Forum web site here.
(http://www.wapforum.org/what/technical.htm)

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

Instructions on how to read a JSP602 leaflet are available here.

Compliance

Stage	Compliance Requirements
Initial Gate/DP1	MOD Projects shall submit a formal declaration that they have read and understood the policy and sought guidance from the SME(s) as required.
Main Gate/DP2	MOD Projects shall reference in their SRD (and MODAF technical views) the specific policy elements contained within this leaflet that are applicable to the infrastructure they are procuring or updating.
Release Authority/DP5	MOD Projects (supported by their equipment suppliers) shall provide evidence of their compliance with the elements of this policy defined within the SRD (and MODAF technical views). Evidence of conformance with standards shall be presented; sources of evidence may include: conformance/compliance certificates provided by equipment suppliers (e.g. under type approval or other assessment regimes), demonstrations, inspection, analysis, tests carried out by suppliers (e.g. Factory Acceptance Tests) and tests carried out at Defence Test and Reference Facilities.