Combined Communications Electronics Board

(CCEB)

Combined Interoperability Technical Architecture (CITA) Rationale and Development Framework

CCEB Publication No. 1007 Issue 2.0

25th January 2001

CITA Working Group

This page is intentionally blank

Record of changes

This is a controlled document under the auspices of the Permanent Secretary of the CCEB.

Additional copies should be obtained through the issuing authority.

In the event of copying locally, each document shall be marked 'Uncontrolled Copy'.

Amendment shall be by whole document replacement.

Proposals for change to this document should be forwarded in writing to the issuing authority i.e. the Permanent Secretary of the CCEB who will then forward it to the current chairman of the CITA Working Group.

Contact

In the event of inquiries with respect to this report, please contact:

Permanent Secretary CCEB

USMCEB

C/- Joint Chiefs of Staff

Room 1B 707, The Pentagon

Washington DC 20301

Phone: 703 614 4684

Fax: 703 693 3322

E-mail goodalkr@js.pentagon.mil

Issue	Date	Details of changes
Draft 0.1	12th February 1998	First draft
Draft 0.2	20th March 1998	Incorporate changes from initial review.
Draft 0.3	10th June 1998	Incorporate changes proposed at 3rd CITA Working Group meeting. (Sent for staffing amongst CCEB groups, nations and other stakeholders)
Issue 1.0	3rd May 1999	Incorporate changes proposed at 4th CITA Working Group meeting following national staffing, and comments from AMH and AIS ISMEs.
Issue 2.0	25 January 2001	Incorporate changes following technology refresh review at 5th CITA Working Group meeting and web-based review.

Executive summary

Background

Recent work amongst some CCEB nations has sought to define technical architectures that will support interoperability between Defence Communications and Information Systems. To achieve these interoperability aspirations in full, certain IT standards[1] would need to be adopted across all CIS. This set of standards has since become known in the UK as the UK Defence Technical Architecture (UK DTA), and in the US as the Joint Technical Architecture[2] (JTA). It is now planned to extend the scope of interoperability between nation boundaries, specifically those members of the CCEB.

Purpose

The purpose of the document is to explain in a logical, step-by-step manner, the process used to develop a technical architecture that will meet the interoperability needs of the CCEB nations. It is aimed at providing Project Managers with a justification of the benefits such an architecture can provide, and providing System Developers with a detailed technical specification of the architecture itself.

This rationale and development framework has resulted from the deliberations of the CCEB nations under a programme of work to define the CCEB Combined Interoperability Technical Architecture (CITA). The objectives of this document are:

- to define the scope of the CITA in terms of the IT services it should encompass;
- to identify candidate services and the rationale behind their selection;
- to identify current and emerging standards that satisfy the selection criteria.

Most recently the CITA has been reviewed in the light of the technology developments that have occurred since its first issue, with experience gained through practical examples of CIS federations and a greater investigation of the constraints experienced by deployed CIS.

ACP 140

---

1 The term 'standard' is used to encompass both *de jure* and *de facto* standards; it is not restricted solely to the products of bodies such as the ISO.

2 The US Architecture framework (as described in the DoD JTA) consists of 3 components, Operational, System and Technical Architectures. This document equates to the Technical Architecture.

An associated document will define the CITA for those services where relevant policy is sufficiently mature to allow a selection to be made. This will be agreed and promulgated as ACP 140. This ACP is derived directly from the CITA Rationale and Development Framework (CRDF). It is intended that ACP 140 will be used as a reference guide by Systems Developers when selecting standards for systems they are building. Further justification for the selection of a particular standard may be gained by recourse to the CRDF. The recent review cycle has resulted in the release of ACP 140A.

Scoping the CCEB Combined Interoperability Technical Architecture

There are many IT services that could contribute to interoperability among CCEB nation CIS; each is a *candidate* for inclusion within the CITA (i.e. for CCEB-wide standardisation). A set of scoping principles has been agreed to govern which of these candidate services should in fact be included within the CITA at this stage. These principles take into account the scale of the requirement for the service, the availability of suitable standards, the feasibility of employing a standard CCEB-wide, and the costs and risks of CCEB-wide standardisation in comparison to more local arrangements for meeting the same interoperability requirement.

The scope of the initial CITA is comparatively limited, loosely equating to a CCEB 'Intranet'[3] (subject to provision of a suitable communications infrastructure). It includes those services in widespread use on the Internet and in commercial Intranets, together with some additional security services essential to military CIS interworking. Although the current CITA services are limited, they will nonetheless support a highly effective federation of interoperating systems. These CITA services could be considered sufficient to achieve CCEB-wide interconnection at NATO level 4; where requirements exist for higher levels, supplementary local technical agreements (e.g. bilateral or nation-specific) will be required.

The CCEB Executive Group has cited NATO level 5 interconnection as the goal; hence there is a need to monitor a number of services for possible inclusion in the CITA in the near and medium-term. These additional services would enhance the capabilities of the CITA by extending the range of interworking mechanisms available, by supporting a broader range of information exchange formats and standards, and by providing the underpinning security framework and services needed to exploit these fully. The CITA developments would reduce the degree to which supplementary agreements are required to achieve the higher levels of interconnection.

Current CITA

A key principle of the CITA is the concept of architectures and their relationships with each other. CCEB nations have differing architectural models but are broadly agreed on three main architectures,

3 A CCEB Intranet is defined as a federation of loosely coupled CCEB CIS, connected by a communications infrastructure, that can interoperate using Internet protocols and standards (e.g. TCP/IP, HTTP & HTML).

the operational architecture[4], the technical architecture and the system architecture. All are required for the development of deliverable systems. The current CITA has achieved the definition a technical architecture that will enable the construction of systems which can interoperate across a CCEB Intranet. Central to this current CITA is an architectural concept based upon the Internet standards and protocols of which the four-layer TCP/IP protocol stack is a primary element.

The resultant CITA profile of standards provides a comprehensive set of interoperability services which can operate over a variety of cable and radio-based communications bearers. The CITA services allow secure messaging and email (with attachments), naming and addressing, document transfers, file transfers and the exchange of specific military data. The CITA services also support web browsing, news groups, video conferencing, and the exchange of multimedia and geospatial data. The full CITA specification is given in Table 7-2~~Table 7-2~~.

Current policy shortfalls

A review of relevant technical policy appropriate to the CITA indicates that whilst effective policy exists for many services, there are gaps in important areas where the suitability of extant policy is questionable. Some policy shortfalls (e.g. data management) have been identified, which if resolved would help avoid costly downstream migration activities or reduce inefficiencies and management overheads. In some cases, the policy shortfalls are already being addressed by bodies outside the CITA working group (e.g. directory schema[5] and general security).

Future Development of the CITA

A consequence of basing the CITA on Internet technology principles is that the technical scope of the CITA will change with time. The CITA specification will need to be developed both for completion and for incorporating changes in requirements, technology and the market place. A development strategy has therefore been identified embracing near-term and future (vision) developments.

4 The operational architecture is split by some nations into business/enterprise and information architectures.

5 It is noted that the updating of ACP 133 is dealing with the issues of directory schema.

List of contents

1. Introduction 1
1.1 Background 1
1.2 Architectures 1
1.3 Relationship between CITA and other Architectures 2
1.4 Objectives of this work 2
1.5 Conduct of the work 3
1.6 Contents of this report 34

2. CCEB Vision and aim of the CITA 67
2.1 Introduction 67
2.2 CCEB Vision 67
2.3 Concept of Operations 78
2.4 Objective of the CITA 78
2.5 Relationship to nation-specific ITAs 89

3. CITA services and standards selection process 1213
3.1 Introduction 1213
3.2 Service identification and standard selection 1213
3.3 Evolution of standards 1314

4. CITA candidate services 1617
4.1 Introduction 1617
4.2 Tabular listing of candidate services 1617

5. CITA scoping principles 2927
5.1 Introduction 2927
5.2 Inter-nation requirements 3028
5.3 Openness 3129
5.4 System boundary issues 3230
5.5 Legacy issues 3331
5.6 Cost, risk and procurement issues 3331
5.7 Interconnection security policy 3432
5.8 System evolution 3533

6. Assessment of scope of the CITA 3735
6.1 Introduction 3735
6.2 Assessment of CITA services 3735

7. CITA Specification 6759
7.1 Introduction 6759
7.2 Overview 6759

7.3 Key Drivers ..... 67~~59~~
7.4 CITA Services Out of Scope ..... 68~~60~~
7.5 Multiple Standards ..... 69~~61~~
7.6 Tabular summary ..... 69~~61~~

8. Applicability and compliance ..... 78~~67~~
8.1 Introduction ..... 78~~67~~
8.2 Scope of CITA applicability ..... 78~~67~~
8.3 Applicability to systems ..... 78~~67~~
8.4 Compliance levels ..... 79~~68~~

9. CITA evolution ..... 82~~71~~
9.1 Introduction ..... 82~~71~~
9.2 Change Drivers ..... 82~~71~~
9.3 New technology developments. ..... 82~~71~~
9.4 New CCEB requirements ..... 83~~72~~
9.5 Resolution of shortfalls in long term technical issues ..... 84~~73~~
9.6 Feedback from projects and external stakeholders ..... 86~~75~~

10. Management ..... 87~~77~~
10.1 Introduction ..... 87~~77~~
10.2 Development of CITA management framework ..... 87~~77~~
10.3 Technical management activities associated with the CITA ..... 87~~77~~
10.4 CITA implementation strategy. ..... 88~~78~~
10.5 Coordination between nations ..... 88~~78~~

11. Summary and Recommendations ..... 91~~81~~
11.1 Introduction ..... 91~~81~~
11.2 Summary of the CITA scope ..... 91~~81~~
11.3 Achievements and benefits of the CITA ..... 91~~81~~
11.4 General issues raised by the CITA ..... 91~~81~~
11.5 Resolution of critical CCEB technical policy shortfalls ..... 92~~82~~
11.6 Emerging areas for CITA ..... 92~~82~~
11.7 Recommendations ..... 93~~83~~

12. Acknowledgments ..... 95~~85~~

13. List of abbreviations ..... 97~~87~~

List of tables

Table 4-1 Candidate services ..... 18~~19~~
Table 6-1 Assessment of scope of the CITA ..... 39~~37~~
Table 7-1 CITA services out of scope ..... 68~~60~~

Table 7-2 Tabular summary.....69~~61~~
Table 8-1 Compliance levels .....79~~68~~

Annexes

A Assessment: supporting information.....91

B CITA Recommended Standards Profiles.....105

1. Introduction

1.1 Background

1.1.1 CCEB publication 1001 (1996), outlines the requirement for the Combined Interoperability Environment. Following this work, at their June 1997 meeting, the CCEB Principals decided to pursue the formulation of a Combined Interoperability Technical Architecture (CITA) as a means of fostering the technical agreements needed to promote interoperability between Allied communications and information systems (CIS).

1.1.2 In this context, interoperability is defined as the ability of CIS from different Allied nations to interconnect, interwork and exchange meaningful information in a secure and timely fashion as determined by business/operational imperatives.

1.1.3 The CCEB Principals set up a specialist Working Group (to be known as the CITA WG) to pursue the definition of the CITA, exploiting Nations' significant expertise in, and recent experience of, developing similar national initiatives.

1.2 Architectures

1.2.1 An architecture is defined by the Institute for Electrical and Electronic Engineers (IEEE) in IEEE 610.12 as the organizational structure of a system or component, their relationships, and the principles and guidelines governing their design and evolution over time. The UK and US have both developed a number of inter-related architecture which together govern the way systems are developed.

1.2.2 The US have defined three architectures as follows:

- Operational Architecture: A description (often graphical) of the operational elements, assigned tasks, and information flows required to accomplish or support the warfighting function. It defines the type of information, the frequency of exchange, and what tasks are supported by these information exchanges.

- Technical Architecture: A minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The technical architecture identifies the services, interfaces, standards, and their relationships. It provides the technical guidelines for implementation of systems upon which engineering specifications are based, common building blocks are built, and product lines are developed.

- System Architecture: Defines the physical connection, location, and identification of the key nodes, circuits, networks, warfighting platforms, etc., and specifies system and component performance parameters. It is constructed to satisfy Operational Architecture requirements using standards defined in the Technical Architecture. The SA shows how multiple systems within a subject area link and interoperate, and may describe the internal construction or operations of particular systems within the architecture.

1.2.3 The UK has defined four architectures. It has Technical and System architectures equivalent to those described above. However it also has a Business Architecture and an Information Architecture which together equate to the Operational architecture described above.

1.2.4 Canada has defined four architectures. There is a Technical Architecture, the same as for the US and UK. There is an Enterprise Architecture which is analogous to the UK Business/Operational Architecture, and an Information Architecture which is the same as for the UK. Finally, there is an Applications Architecture which is a logical architecture corresponding to the US and UK System Architectures.

1.2.5 A comparison of current CIS architecture frameworks is given below.

UK CIS Architectures	US CIS Architectures	Canadian CIS Architectures
Business/Operational	Operational	Enterprise
Information		Information
System	System	Application
Technical	Technical	Technical

1.3 Relationship between CITA and other Architectures

1.3.1 The CITA equates to the Technical Architecture as defined above. It identifies the list of services that may be required by a system in order to interoperate with other systems; furthermore it specifies the standards that should be used when implementing those services.

1.4 Objectives of this work

1.4.1 The first issue of this document achieved its primary aim of producing the first CITA and detailing the process for updating of the CITA. ACP 140 was produced from this process and contains the recommendations for a profile (or profiles) of CIS standards and/or products that will support essential requirements for interoperability among Allied CIS. This second issue is the natural progression of the process defined within this document. Its purpose is to review and

update the service areas that are within the scope of the CITA together with profile of standards. This review is driven by changes in inter-nation requirements, experience gained from the federation of coalition CIS, technological progression, particularly in the Internet standards, and a greater investigation of the constraints that must be managed when CIS are deployed.

1.5 Conduct of the work

1.5.1 The initial programme of work was conducted through a series of meetings of the CITA Working Group over a 12 month period. The CITA Working Group identified a four stage approach which forms the basis of this report. These are:

- identification of candidate services;
- formulation of scoping principles;
- assessment of the scope of CITA for each service;
- selection of standards and guidelines to be included in ACP 140.

1.5.2 In accord with the above the CITA WG took into consideration nation's existing technical architectures, in particular the US DoD JTA and the UK DTA. Additionally it also considered the ABCA ITA.

1.5.3 As originally envisaged the initial specification needed to be further developed through the establishment of a permanent working group. The permanent working group met in March 2000 to review the programme of work and refresh the CITA. This meeting was followed by a period of 'electronic' working. The document review process was continued through a dedicated web site (hosted by the UK) known as the 'CITA Collaboration Tool' (CCT). This provided a mechanism for hosting on-line discussions of the CITA working group's documents. The process was supported by a number Video Tele-Conferences (VTCs) coordinated by Canada (through its VTC bridge).

1.5.4 The review period having been completed, the work has resulted in the second issue of this document, i.e. the CITA Rationale and Development Framework (CRDF) and the production of ACP 140A (the second issue of ACP 140.

1.6 Contents of this report

1.6.1 This document is organised into the following chapters based around the processes involved in developing the CITA:

- Chapter 1 (this chapter) entitled *Introduction* describes the background to, and objectives of, this rationale and development framework;

- Chapter 2 entitled *CCEB Vision and aim of the CITA* states the CCEB vision for CIS, and identifies the consequent aim and objectives of the CITA;

- Chapter 3 entitled *CITA services and standards selection process* explains the different stages of the method used to select the services to be included in the CITA and which standards should be adopted;

- Chapter 4 entitled *CITA candidate services* identifies the full set of candidate services that could potentially be standardised to support the objectives of the CITA;

- Chapter 5 entitled *CITA scoping principles* gives a set of principles by which the scope of service standardisation within the CITA is determined;

- Chapter 6 entitled *Assessment of scope of the CITA* applies the principles to each CITA candidate service to establish those for which CCEB-wide standardisation is both necessary and feasible; the result is the definition of the technical scope of the first CITA specification, and identification of potential developments;

- Chapter 7 entitled *CITA Specification* identifies the standards, where they exist, that satisfy the criteria for inclusion in the first CITA specification;

- Chapter 8 entitled *Applicability and compliance* defines the scope of the CITA applicability and the compliance levels for system interoperability;

- Chapter 9 entitled *CITA evolution* defines the key drivers that influence the evolution of the CITA and identifies the main areas of emerging technology;

- Chapter 10 entitled *Management* defines the management framework and the necessary actions required to ensure that future development of the CITA is in line with technological advances;

- Chapter 11 entitled *Summary and Recommendations* summarises the CITA scope and presents the main recommendations emerging from this work;

- Annex A contains supplementary explanatory material in support of the assessment in chapter 6;

- Annex B contains the detailed CITA Specification and rationale.

This page is intentionally blank

2. CCEB Vision and aim of the CITA

2.1 Introduction

2.1.1 This chapter states the CCEB vision and goes on to identify the consequent aim and objectives of the CITA. In practice the vision describes CCEB's aspirations and thus sets the strategic direction for CCEB CIS.

2.2 CCEB Vision

2.2.1 The CCEB vision statement adopted by the Principals which describes the goal environment is:

"The CCEB is committed to maximising the effectiveness of combined operations by the definition of a Combined Interoperability Environment. This environment will enable users to share, creatively apply and add value to collective information and knowledge, constrained solely by policies defined by originators and recipients." [CCEB Publication 1 Ver 3.1 dated 11th Aug 2000]

2.2.2 The Combined Interoperability Environment goal is to establish an interoperable CIS capability, that should be achieved in an affordable and cost-effective way, able to support all nations' defence requirements.

2.2.3 Individual CIS will be designed, procured and maintained to meet the requirements of their user population, but will also acknowledge obligations to support CCEB objectives. In particular, CIS will be widely interconnected, provide common services to support exchange of information, and be managed autonomously but paying suitable cognisance to wider needs. CCEB CIS will thus exist in a loose federation, with each system fulfilling its own mission, but drawing on services provided by other systems, and in turn providing services needed by others.

2.2.4 Subject to security rules, any user should be able to access required information, and will do so in a consistent and familiar way irrespective of task or location. CIS should support this by providing consistent mechanisms to ensure that entitled users are able to determine the existence and location of information and transfer that information where necessary.

2.2.5 Underpinning the end systems will be a seamless, world-wide, efficient and survivable communications infrastructure supporting information transfer across the whole CCEB defence community, interfacing as required with other Allied and civil communications systems.

2.2.6 CIS should be based on standard commercial hardware and software components wherever possible. Specific development will usually be limited to military-specific components and specialised integration software.

2.3 Concept of Operations

2.3.1 Fundamental to the definition of interoperability is an understanding of the operational environment within which the CCEB nations will operate and in which interoperability must be achieved.

2.3.2 The operational environment of the future is perceived to be one of coalitions, flexible in their constitution and unlikely to be constrained to CCEB members. Partners will not have common procedures and operational techniques. The operational environment will also need to take into account civil and national influences and the integration of functional elements at all levels of the organisational structure.

2.3.3 The essence of combined interoperability is the ability to integrate command and control systems within this coalition structure. This requirement is the ability to share and actively exploit common information while dynamically developing processes and procedures that are appropriate to the existing coalition.

2.4 Objective of the CITA

2.4.1 The objective of the CITA is to provide the CIS standards necessary to achieve the above vision. The primary aim is to facilitate interoperability among CCEB nation's CIS; that is to allow CIS, supporting the needs of different elements within the CCEB Nation's business, to exchange information and other services in a timely and secure manner, as determined by business[6] and operational imperatives.

2.4.2 It should be noted also that application portability, could in certain circumstances contribute to interoperability, however there is no apparent requirement for routine porting of applications between systems of different CCEB nations; nor is it judged feasible to undertake, on a CCEB-wide basis, the invasive standardisation that would be needed to support such a requirement.

2.4.3 In support of the above aim the following interoperability objectives are set for the first CITA specification:

---

6 Some nations regard 'operational' systems as those pertaining to war-fighting only. Others regard 'operational' as including non-operational CIS as well. The term 'business' is included here to ensure that non-operational CIS are explicitly included.

- **Interconnection.** To ensure that end-systems are capable of direct electronic attachment to one another or to a common logical network.

- **Interworking.** To ensure that systems employ compatible mechanisms for the exchange of services and data.

- **Information exchange.** To ensure that users and applications on different systems can attach a common meaning[7] to data exchanged between them.

2.4.4 These objectives equate to a set of dependent layers with Interconnection being the lowest, most fundamental layer and Information exchange being the highest layer.

2.4.5 In meeting these objectives it is vital that all systems adhere to a common security framework so that each affords appropriate protection to information held within the CCEB CIS federation[8].

2.4.6 In practice the current CITA will allow messages, attachments and other forms of electronic information (including data, audio, video and fax) to be 'pushed' from one CIS to another. Messages may also include requests for one CIS to send specific data items. This equates to NATO level 4 interconnection.

2.4.7 The emerging CITA will additionally permit CIS to access the processing and other resources available on remote systems. This equates to a sharing of services as well as information and includes the ability to 'pull' information from one CIS to another. This equates to NATO level 5 interconnection.

2.5 Relationship to nation-specific ITAs

2.5.1 Clearly, the Nation Specific ITAs (and any alternative forms of local agreement relevant to other nations) must embrace the CITA: This concept is depicted in figure 2.1 below.

---

7 This is not restricted to metadata definitions and models but included any data that contains information that must be interpreted in order to be understood by humans or applications (e.g. HTTP format tags).

8 The CCEB CIS federation refers to a collection of systems, both fixed and deployed, connected together such that they can exchange information across the Intranet of which they form a part.

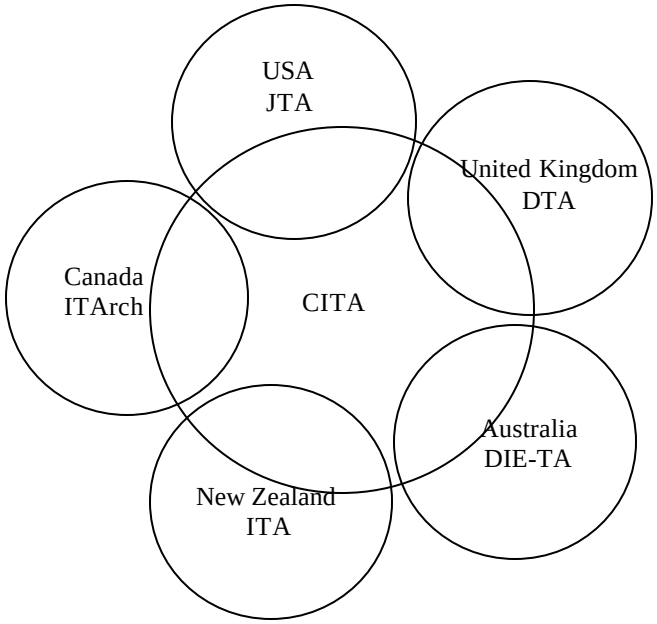

Figure 2.1: Scope of the CITA in relation to other NSITAs

2.5.2 The technical scope of the CITA will establish where the boundary between it and nation-specific ITAs lies. This will depend largely on the interoperability mechanisms CITA aims to employ. A service will be deemed *outside* the CITA if the need to use it (and hence standardise it) arises solely from requirements within individual nation boundaries. Conversely, a service is a *candidate* for standardisation within the CITA whenever there is a significant requirement for exchange of that service between CIS from different CCEB nations.

2.5.3 A balance must be established between the benefits and restrictions of standardisation. This will be the case when a limited number of CIS are involved and an ad hoc bilateral, or multilateral agreement would suffice. The *principles* by which it is proposed this and similar decisions should be made are discussed in Chapter 4.

2.5.4 Local system issues will prevail irrespective of where the CITA/nation-specific ITA boundary is drawn; the combination of the CITA and a nation-specific ITA does not constitute a complete specification of a system. At the very least, each system will offer applications specific to the needs of its local users.

2.5.5 Furthermore, there will be locally required infrastructure services for which standardisation (either within the CITA or a nation-specific ITA) would serve no useful purpose; in these cases,

CIS will select system elements according to purely local requirements or perhaps in accordance with sector level (i.e. Land, Sea or Air) preferences (e.g. ABCA agreements)[9].

[9] Of course, what may start out as local agreements may find wider utility. In this case, these local agreements may be adopted by and subsumed the CITA depending on the scale and scope of their applicability. The overall objective is to move towards commonality.

This page is intentionally blank

3. CITA services and standards selection process

3.1 Introduction

3.1.1 This chapter outlines that process used by the CITA Working Group to first of all select a candidate set of IT services necessary to achieve interoperability, and then define standards for each of the selected services.

3.2 Service identification and standard selection

3.2.1 In the context of this document a service refers to any facility that provides functionality or information to other entities. Standards are the agreed methods by which a service is provided. In simple terms the service defines *what* is provided and the standard defines *how* it is provided. For example, the HTML document transfer service is performed using the HTTP standard.

3.2.2 The CITA standards selection process consists of applying four 'stages' as depicted below in figure 3.1. The first three stages are concerned with identifying the set of services that must be provided to achieve the interoperability vision. The fourth stage selects the standard or standards appropriate for each service.

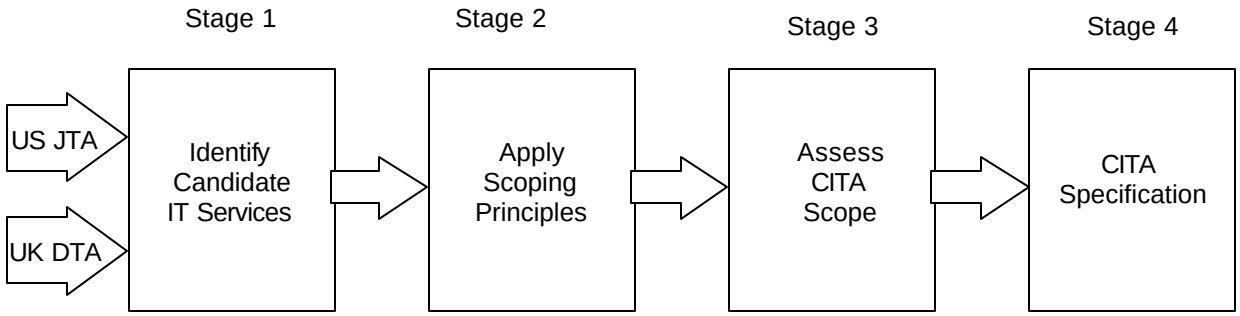

Figure 3-1: Overview of CITA Standards Process

3.2.3 The starting point for the selection process is an aggregation of services taken from the US JTA and the UK DTA. These have been identified as candidates for standardisation within the CITA.

3.2.4 The first stage involves the selection of a subset of services that were considered relevant to the interoperability modes of interconnection, interworking and information exchange defined in Chapter 2. The table in Chapter 4 presents the assessment of each service against the level of interoperability it provides. The inclusion of a function or service at this stage does not necessarily imply that it falls within the scope of the CITA.

3.2.5 The second stage involved the definition of a set of the selection principles that should be applied to each service. These principles make it possible to determine whether a service is in scope or out of scope. The selection principles are defined in Chapter 5.

3.2.6 The third stage involves the examination of each service against the selection principles defined in chapter 5. An assessment is presented in chapter 6 examining each of the candidate services on the basis of the principles to decide whether it is necessary or feasible to undertake standardisation within the CITA.

3.2.7 The fourth stage involves the selection of one or more standards for each of the candidate services. Standards are selected on the basis of those which provide the best combination of:

- openness (as defined in paragraph 5.3),
- wide product support (particularly through COTS products),
- are leaders in terms of market uptake.

3.2.8 In some cases the market position of a number of products that support a de facto standard has been deemed more significant than the openness of a de jure standard.

3.2.9 Standards that are not relevant to interoperability (e.g. those areas dealing with software development); are not considered further in detail in this document. However, in recognition of the fact that requirements may change and other considerations such as application and people portability may become important, these 'place holders' have been retained to ensure that they are always formally reviewed.

3.3 Evolution of standards

3.3.1 The CITA Working Group recognises the fact that rapid advancement in commercial technology inevitably has an impact on standards. For the CITA to remain relevant a process of evolution is necessary which will:

- continuously review the candidate services,
- monitor the requirements for services,

- review, and update where necessary, the specified standards.

3.3.2 Furthermore, when standards change and evolve, it is essential that compatibility issues are fully taken in to account. Poor evolution of the CITA risks the introduction of incompatible and conflicting standards which would only serve to reduce interoperability and increase the cost of remedial action.

This page is intentionally blank

4. CITA candidate services

4.1 Introduction

4.1.1 This chapter forms the first stage of the selection process. A range of IT services taken from the US JTA and the UK DTA have been identified as candidates for standardisation within the CITA. These candidate services are identified in this chapter, classified in terms of the level of interoperability they provide. The results are presented in Table 4-1~~Table 4-1~~.

4.2 Tabular listing of candidate services

4.2.1 The following table identifies which of the IT services in each category qualify as candidates for subsequent consideration. For brevity the following nomenclature has been used:

- 'All' indicates that all IT services listed in this category qualify as candidates in support of that specific CITA objective;

- 'All except as noted' indicates that all services in this category qualify other than those listed explicitly in the table under a different CITA objective or assessed not to be relevant to interoperability (i.e. under a different table column).

4.2.2 Additionally, some services may appear several times within the breakdown because they can legitimately be considered part of more than one category. These cases are highlighted in the table, with the relevant function or service being addressed in the most appropriate place.

4.2.3 As mentioned earlier in section 2.4 and to aid understanding of Table 4-1~~Table 4-1~~ the following interoperability levels have been set for the first CITA specification:

- **Interconnection.** To ensure that end-systems are capable of direct electronic attachment to one another or to a common logical network.

- **Interworking.** To ensure that systems employ compatible mechanisms for the exchange of services and data.

- **Information exchange.** To ensure that users and applications on different systems can attach a common meaning[7] to data exchanged between them.

This page is intentionally blank

Table 4-1 Candidate services

Section/category	Description	Relevant CITA objectives			Comments
		Information exchange	**Interworking**	**Interconnection**	
1: Operating System Services	Standards for the services provided by computer operating systems and the means of accessing them by user applications.	**N/A**			Not relevant. Relevant to application portability and to cost/risk management.
2: User interface services	This category covers a miscellany of standards relevant to the Human-Computer Interface, including look and feel standards/conventions, APIs for windowing systems, desktop managers plus desktop hardware and operating system environments. It includes remote presentation protocols (e.g. X11) and inter-process communication protocols (e.g. DDE) which are also listed under Distributed Computing below.	**N/A**			The majority of standards in this category are not relevant to any CITA objectives but to applications portability or person portability. Those standards that are potentially relevant (i.e. remote presentation and IPC) are addressed individually under Distributed Computing below.
3: Network services					
Communications applications	These are communications-related applications operating at or above layer 7 of the ISO OSI reference model.		All		These applications were intended for use with the ISO OSI 7 layer protocol stack. To run over TCP/IP they require the IPS equivalents of OSI layers 5 through 7 (see below).
Messaging	Store-and-forward transfer of messages.		All		
Directory services	Services for the provision of information relating to all forms of communications and information services including the support of messaging and security services.	See (i)	See (ii)		(i) Directory schema; object and attribute definitions; interchange format for directory data (ii) Directory access, shadowing and chaining protocols
Name and Addressing services	Services for resolution of computer or server names into specific addresses.		All		Includes services to translate between addresses used in different sub-networks.
Remote terminal services	Protocols and applications that enable remote terminals to connect into a system. They include both OSI application-layer standards and their Internet Protocol Suite (IPS) equivalents. Such connections typically emulate character-based terminals and are used to provide access to legacy systems.				
File transfer services	Protocols and applications to provide a file transfer facility. They include both OSI application-layer standards and their IPS equivalents.		All		
Communications upper layers (i.e. OSI RM layers 5-7 and IPS equivalents)	Services and protocols.		All		OSI applications over TCP/IP lower layers are included.

Socket services	This category includes APIs providing access to Internet protocols (e.g. WinSock) and associated applications.	N/A	WinSock API and comparable APIs are not relevant to CITA objectives. These may be relevant to application portability.

Section/category	Description	Relevant CITA objectives			Comments
		Information exchange	Interworking	Interconnection	
4: Communications					
Networking					
Telephony	Services for voice encoding across both analogue and digital dial-up connections. Includes modem services.			All	
Wide area networking	Standards for the transfer of data across wide area networks including X.25, Frame Relay, ISDN, B-ISDN (ATM) and SONET			All	
Coalition WAN	Standards for the interconnection of network components forming the Coalition wide area network				
Local area networking	Self-explanatory.			All	
Point-to-point services	Services providing full duplex, synchronous or asynchronous network connections over a serial line.			All	
Tactical data link services	Tactical data links provide the means for exchanging tactical information used for battle management.			All	
Combat net radio	Combat Net Radio (CNR) provides survivable, mobile communications on the battlefield using radio equipment operating in the HF, VHF and UHF bands.			All	
Network Interconnection					
Internetworking	Standards for the transfer of data across LAN/WAN and LAN/LAN boundaries.			All	
Router services	Routers are used to interconnect networks of differing types, including sub-networks and end systems.			All	
Transport services	Services providing user access to internetworking services and end-to-end quality enhancement			All	
Bearers					
SATCOM	Standards for the transfer of data across SATCOM links including UHF, SHF and EHF.			All	
Radio	Standards for the transfer of data across Radio links including VLF, LF, HF, VHF, UHF and SHF.			All	
Cable	Standards for the transfer of data across copper and fibre links including Optical, Shielded Twisted Pair and UTP			All	

Section/category	Description	Relevant CITA objectives			Comments
		Information exchange	Interworking	Interconnection	
5: Distributed computing					
Distributed database management services	Services for maintenance or querying of databases distributed over multiple physical locations.				These are listed under nation level data management and are addressed there.
Distributed Process (RPC)	Remote procedure call (included in this category are the other forms of inter-process communication).		All		
Remote presentation services	Protocols permitting graphical user interfaces to execute remotely from the client application (e.g. X11).		All		
Distributed file services	File sharing protocols.		All		
Distributed time services	Protocols for synchronisation of system clocks.		All		
Distributed print services	Protocols for transfer of print jobs from client to spooler/printer.		All		
Distributed transaction processing services	Services for the management of transactions involving participants on different end-systems.		All		
Distributed object services (object middleware)	Services for location of, or access to, objects when distributed over a network.		All		
Distributed system management services	Services for the coordinated management of various distributed components within a system.		All		
6: Data management services					
Remote data access	These are mechanisms that allow clients to access data on remote database servers in a client/server environment.		All		
CCEB level data management	This category covers what would normally be described as data management. It includes data models plus associated metadata standards and data management procedures.	All			
Project level data management					
Data dictionary services	These are software development support tools that facilitate the management and use of project data dictionaries.	N/A			These are not relevant to CITA objectives but are relevant to other objectives (such as application portability or reuse).
Database management system services	These are the facilities provided by a conventional RDBMS.	N/A			These are not relevant to CITA objectives but are relevant to other objectives (such as application portability or reuse).
Distributed data services					
Database to database replication	These are mechanisms for replication of data between DBMSs, such as provided by modern commercial DBMS products.		All		

Standard data products	These are specific data sets developed to support the functions of particular areas of the business. The data products cited are geospatial, Hydrographic and Aeronautical data sets.	All	

Section/category	Description	Relevant CITA objectives			Comments
		Information exchange	Interworking	Interconnection	
7: Data interchange					
Business-transaction-oriented data interchange standards	Specific text- or bit-oriented formats for representation of business-related data.	All			
Additional military message formats	Encodings of military-specific information in structured or unstructured form. Structured formats include both binary (bit-level) encodings and text-based (machine and human-readable) messages.	All			Business-transaction-oriented data interchange standards do not presently include a number of relevant military message formats so these have been included here as an additional category.
Document interchange standards					There are a multitude of different document interchange formats. For the purposes of this analysis, document interchange formats have been divided into two categories, OA and hypertext. This category also includes HTTP, the hypertext transfer protocol.
Office Automation interchange formats	Formats used for interchange of documents between OA tools (word processor, spreadsheet, etc.).	All			
Hypertext interchange formats	Formats for representation and transfer of hypertext documents.	All			
Hypertext transfer protocols	Protocols used for the transfer of hypertext documents between systems, including selective transfer for ‘browsing’.		All		
Character sets and alphabets	Binary encodings used to represent alphanumeric characters and special characters used in foreign languages or technical literature.		All		
Encoding standards	Standards for encoding of binary or structured data, usually for transfer via a communications medium. This category covers ASN.1 and its encoding rules, UUENCODE and MIME.		All		
Object interchange standards	Data formats relevant to the encoding of object structures used in distributed computing. The specific formats cited are OLE and OpenDoc.		All		These services are related to those listed in the distributed computing category.
Graphical/still image data interchange standards (including geospatial and fax data)	This category covers a wide range of standards used for representation of still image and graphic data, including geospatial and imagery referenced data formats. It also includes the fax standards (group 3 and group 4) for representation and transfer of page images.	All			Group 3 and Group 4 fax standards are only relevant to communications.
Moving image and audio/visual data interchange standards	As above but for moving images. It also includes standards for video conferencing and video telephony.	All			ITU Video standards are only relevant to communications.

Audio data interchange standards	As above but for sound. It also includes various standards relevant to telephony.	All (See comment)	All	ITU audio standards are only relevant to telecommunications. Audio information can be stored and replayed digitally using specific file formats (e.g. .AU, WAV, AIFF) ; these are relevant to the Information exchange mode of interoperability.

Section/category	Description	Relevant CITA objectives			Comments
		Information exchange	Interworking	Interconnection	
7: Data interchange (cont.)					
File compression	Standards for the extraction and encoding of compact file representations.		All		
Multimedia and distributed real-time service data interchange standards	See comment.				See relevant data interchange category above. (All standards listed in this category are already listed in one of the categories above.)
Page description	Standards for describing page layouts for submission to print or display devices (e.g. postscript).	All			
Miscellaneous data interchange standards	This is a catch-all category of standards not listed elsewhere. It includes: - CASE interchange formats - graphics meta-formats (e.g. Windows Metafile)	All except as noted.			CASE DIF not relevant to CITA objectives.
8: System and Network Management					The standards are organised here into two broad categories, system and network management.
System management	Services supporting the management of end-systems, including user administration, configuration management, fault management, security management, etc.		All		
Network management	Services supporting the management of networks under the control of end-systems or within the wide-area communications infrastructure.			All	
9: Software Engineering Services	This category mainly covers standards for the system/software lifecycle processes and associated tools but also includes standards for programming languages and their bindings				Not relevant to any CITA objectives. Software engineering services are relevant to other objectives such as value for money or application portability
Languages and bindings	See Above				
4GLs and CASE tools	See Above				
Integration	See Above				

Section/category	Description	Relevant CITA objectives			Comments
		Information exchange	Interworking	Interconnection	
10: Graphics					This category includes a miscellany of graphics-related standards, many of which are also listed elsewhere in the guides. For clarity, standards in this category have been grouped into a number of areas which are described separately below.
Graphics programming languages and APIs	Languages or language bindings to facilitate the production of graphics-based applications software.				Not relevant to CITA objectives. Relevant to application- or person portability.
Page description or display languages	Languages for describing page layouts for submission to print or display devices.				Many of these are relevant to CITA objectives but are also listed as data interchange standards above.
Application software packages having a drawing capability	Examples include CAD/CAM packages, OA graphics packages.				Not relevant to CITA objectives. Relevant to application- or person portability.
Military symbology standards	Standards for representation of military symbols (usually on map overlays).	All except as noted			Some relevance to CITA objectives. The symbols are relevant only to application- or person portability, however the underlying encoding information, which defines the meaning behind the symbols, is relevant to interoperability.
Remote presentation services	Protocols permitting graphical user interfaces to execute remotely from the client application (e.g. X11).				These services are also listed in the distributed computing category and are addressed there.
11: Internationalisation	Internationalisation services are those standards and conventions that facilitate the use or re-use of systems or software within different National or cultural contexts. They cover a broad range of Internationalisation standards which can be loosely categorised as character sets, specific data representations and Internationalisation aspects of system interfaces (mainly HCI).				These services are largely irrelevant to CITA objectives, with the exception of character sets (which are covered under the data exchange category above). These standards are primarily relevant to person portability.

Section/category	Description	Relevant CITA objectives			Comments
		Information exchange	Interworking	Interconnection	
12: Security Services					The area of security services is not yet explored in detail. This report adopts the following categorisation of security services relevant to interoperability. Each service is defined in the context of its application to interaction between systems.
Authentication	Authentication services are those services supporting the reliable identification of individual users or groups of users of one system attempting to access services or information provided by another system.		All		
Access control	Access control services are those services supporting the exercise and promulgation of access rights for service/information exchange between systems based on user identity, role, group, clearance or other privilege attributes. This includes standards for security labels where these are used (e.g. message exchange).		All		
Key management and distribution	Services supporting the management and distribution of cryptographic keys.		All		
Confidentiality and integrity	Services supporting the confidentiality and integrity of information/services exchanged between systems.		All		
Accounting and audit	Services supporting the recording and analysis of security-relevant events involved in the exchange of services/information between systems.		All		
Non-repudiation	Services supporting the verification of provision/acceptance of services or information between systems.		All		
Security domain mediation	Services supporting the secure exchange of services between systems operating under differing security policies or within separate security domains.		All		

Section/category	Description	Relevant CITA objectives			Comments
		Information exchange	Interworking	Interconnection	
13: Support application software	This category covers general-purpose or utility applications software. A variety of application types are included under this heading . Those covered explicitly under this heading are OA applications and those categorised as transaction processing applications (OSI application layer service elements).	All			
14: Collaborative Computing					Collaborative computing services identified here include a number of specific services potentially relevant to interoperability.
Workflow services	Services supporting the automated transfer of documents or other information between users or organisations on the basis of a predefined business process.		All		
On-line wide area publishing	Services supporting group access (read/write) to structured or unstructured information on the basis of subject area or other categorisation.		All		
News group services	Information transfer services designed to notify registered subscribers of updates occurring in news groups and transfer relevant information		All		
Whiteboarding	Services supporting the sharing of displays across a network.		All		
15: Special application software	This category covers system- or mission-specific applications software which would only be expected to be found on systems performing a similar role.	See comment			Potential relevance to any of the CITA objectives can only really be assessed on a case-by-case basis for these applications.
Geographic Information Systems (GIS)	Applications providing services relating to the storage, retrieval, querying and transfer of geographic data and items that are referenced to a geospatial grid.	All			
Track Management	Applications providing services relating to the storage, retrieval, correlation, update and query of tracks.	All			
Alert services	Information transfer services designed to support the rapid or widespread distribution of information, usually having great operational significance.		All		Alert services are often cited as being candidates for standardisation as an interoperability mechanism.

5. CITA scoping principles

5.1 Introduction

5.1.1 This chapter states a set of principles that has been used to govern the scope of technical standardisation attempted under the CITA. These principles form the second 'stage' described in Chapter 3.

5.1.2 The statement of objectives of the CITA given in Chapter 2 indicates that its broad technical scope is determined by the requirements for information and service exchange *between* nation's CIS rather than within them[10]. A decision to standardise a service or mechanism within the CITA must, however, be based on more than merely whether that service *could* be exchanged between CCEB CIS. It is essential that, in deciding the scope of the CITA, a balance is struck between the benefits of adopting CCEB-wide standards and the disadvantages that standardisation could entail. In striking this balance, therefore, it is also necessary to consider:

- **feasibility**: the technical feasibility of exchanging a service or employing a particular mechanism across CIS, particular in a secure environment;

- **scale of use:** the extent to which that service or mechanism is employed to meet requirements for information and service exchange between systems in different business domains[11];

- **competing drivers**: business and operational imperatives that may militate against standardisation, such as devolution of control, avoidance of lock-in, transfer of risk, cost, etc.

5.1.3 Bearing these three considerations in mind, the scoping rules have been formulated around seven key principles. Some of the key principles are further subdivided for added clarity when applying them to each of the candidate services. The seven key principles are:

- Inter-nation requirements

- Openness

---

10 Of course, any service standardised within the CITA, could also be employed to meet intra-nation interoperability requirements; however, agreement on more sophisticated interoperability mechanisms would be legitimate within a nation to meet nation-specific requirements.

11 A service or mechanism employed on a large scale within a particular nation is a candidate for standardisation within that domain (e.g. as part of a nation-specific technical architecture or other nation-specific policy).

- System boundary issues
- Legacy issues
- Cost, risk and procurement issues
- Interconnection security policy
- System evolution

5.1.4 There are legitimate reasons other than interoperability for standardising a particular aspect of CIS; common reasons include people portability (i.e. where a standard promotes a common look and feel). Moreover, many standards are simply framework documents that allow individual projects to state their requirements concisely in procurement specifications by quoting particular parameters permitted within the standard. Such standardisation drivers are not considered further in this report.

5.2 Inter-nation requirements

5.2.1 *The CITA should standardise only those services that are relevant to CCEB nation's CIS interoperability.*

There are many IT services that are or could be routinely provided within a nation or an individual system, but which are not relevant to CCEB nation's interoperability. An example of the latter might be a distributed print service (i.e. the ability of one computer to issue a print job to a networked printer or to another computer for spooling). This principle states that services not relevant to CCEB nation's interoperability should be excluded from the scope of the CITA.

5.2.2 *The CITA should only standardise services where there is evidence of a present or near term requirement for such standardisation.*

The scope of the CITA, in terms of the services it specifies, will inevitably change over time[12]. There is a temptation to standardise services *just in case* a future inter-nation requirement for their use should arise. Although there may be instances where such pre-emptive action is beneficial, the main effect of such a policy is to foster unnecessary standardisation.

[12] An example of this might be a protocol for dynamic downloading of executable software from one system to another. Few would have predicted the need to standardise such a protocol a few years ago, whereas this is now becoming commonplace in Intranet applications.

5.2.3 *The CITA should standardise services only where there is sufficient scale of benefit to be gained.*

There are many standards that could be potentially useful in achieving CCEB nation interoperability but their applicability is limited to particular functional areas or environments. Also there may be functions or services needed only by small groups of systems, the standards for which could thus legitimately be chosen locally. This principle states that unless there is clear benefit from widespread standardisation across CIS (with the potential cost and risk penalties of enforcement) the CITA should be silent and the specification of standards left to a more local level.

5.3 Openness

5.3.1 *The CITA should not attempt to standardise a service for which there is no effective open standard unless the business advantages of adopting a non-open solution can be shown to outweigh the likely disadvantages.*

Products exist that allow IT systems to exchange a wide range of services to achieve a high degree of interoperability; however, there are comparatively few areas where genuinely open, vendor-neutral solutions exist. Furthermore, even where open solutions do exist, product support can be poor and the products that are available much less capable than corresponding proprietary solutions.

Ideally, standardisation of a service should only be undertaken where there is an effective open solution[13]. However, there will remain circumstances where effective open solutions do not exist, yet the business benefits of standardisation would be significant[14].

In practice, to scope the CITA it is necessary in some areas to trade-off the business benefits of having a comprehensive CITA with the numerous risks (e.g. lock-in, loss of project design freedom) associated with CCEB-wide adoption of non-open solutions. Specifically, it will be necessary to consider whether:

- the strength of the business requirement is sufficient to justify the adoption of a proprietary solution within the CITA (forcing every participating end-system to follow that approach);

13 Formally, to be classified as ‘open’ a standard must exist in the form of a specification that is controlled and maintained by a public body. In some cases an acceptably open standard may include MIL-STDs, STANAGs and other non-commercial standards.

14 One possible example could be a network security protocol; the commercial market has not yet identified a de facto standard but the capability is so critical to interworking between CCEB Nation’s Defence systems that selection of a single product for CCEB-wide use may be justified.

- standardising on a less capable but vendor-neutral solution would prevent projects from selecting more powerful, but proprietary, technologies essential to meeting their local requirements.

The following criteria are suggested to determine whether or not a solution qualifies as being *acceptably open* from a CITA perspective:

- there is an effective de jure or de facto documentary specification. To be effective, there must be widespread market support for the specification. Among competing specifications it should be the dominant specification and have a substantial share of the market;

- there is a mainstream product achieving substantial market dominance. Examples of this could be the Windows NT operating system or the MS Office OA suite. Although these embody proprietary standards their overwhelming market dominance would force any serious competitor to provide a route to ready upgrade, mitigating the risks of lock-in;

- there are several interchangeable, competing products providing the same service. This ensures that lock-in can be avoided and has the subsidiary benefit of maintaining a competitive environment.

5.4 System boundary issues

5.4.1 *As far as possible, conformance with CITA standards should be confined to requirements to provide specified services at the interface between systems or nations.*

The CITA should be confined to specifying those characteristics of systems that are necessary to achieve allied nation CIS interoperability (this was embodied in an earlier principle). It will often be sufficient that systems comply with a standard at their external boundaries; interoperability does not necessarily demand that services conforming to the same standards are used internally. It is highly desirable that, to the maximum extent possible, intra-system mechanisms and their associated standards should remain a local decision.

Conformance to a specification at the boundary will, however, often mean that certain requirements *do* need to be satisfied internally. For example, the CITA might demand that a certain external schema is used when relational information is exchanged between systems; the schema used internally need not be identical to this but it must clearly be rich *enough* that data can be accurately translated between internal and external formats.

5.4.2 *Systems should be capable of meeting CITA external interface specifications, but this should not preclude the agreement of additional private interfaces between two or more systems if these satisfy local[15] requirements more effectively.*

Any system offering a service within the scope of the CITA is obliged to offer external interfaces conformant with the CITA specification. This allows any other system to interoperate readily if it also offers a compliant interface. However, there will remain circumstances where additional, privately agreed interfaces may be more effective in meeting specific local interoperability requirements, either in terms of performance or cost-effectiveness. In these cases, the CITA should not force projects to adopt a sub-optimal solution where it can be shown that alternative private arrangements are more effective. (It is re-iterated, however, that every system within the scope of the CITA *must* always offer CITA conformant interfaces, in addition to any private interfaces.)

5.5 Legacy issues

5.5.1 *Existing standards implemented in legacy systems should be preferred if they are equal in all other respects to other candidate standards.*

There are two reasons why standards already implemented in legacy systems might be preferred: first, they are demonstrated; second, and more importantly, migration of legacy systems to a new standard could be infeasible or prohibitively expensive. Standards that are already implemented should form a starting point, unless these are judged no longer appropriate. Subject to their continuing validity, this will lead to a preference for standards implemented in legacy systems. This principle ensures that change is not made purely for the sake of change: however, the CITA is in essence a forward-looking document.

5.6 Cost, risk and procurement issues

5.6.1 *The CITA should not standardise services where this would unacceptably interfere with legitimate local project management or procurement freedoms.*

The objectives of the CITA require that certain services are standardised across CCEB CIS. However, projects will need to be individually responsible for specifying local requirements and managing the risks associated with their implementation. This inevitably means that projects need considerable local design freedoms. Indeed, procurement policy will often demand that certain decisions are placed with the supplier, or that product choices are made as part of a competitive project phase. CITA

15 In this context 'local' can mean between two CIS from a single nation, or between CIS of different nations.

standardisation aspirations must therefore be moderated by genuine needs for local project management and control. The effect of this principle is to limit the standardisation of services exchanged between nations so that constraints on projects are contained within acceptable bounds.

With many standards selection initiatives there is a risk that an inappropriate standard is adopted (as happened with OSI, for example). There is therefore an obligation on the CITA to adopt market-led standards for which the risk of adoption is minimal. Even so, the pace of technology change is such that the chances of successfully predicting market leading products or technology for more than a year or two ahead are small.

5.6.2 *The CITA should standardise services only where, to meet the same interoperability requirement, the resultant cost reductions outweigh the costs of the standards making and enforcement processes themselves.*

Even if, *to meet the same interoperability requirement,* CCEB-wide standardisation of a service reduces whole-life costs compared to the costs of local arrangements, the costs of the standards making and enforcement processes themselves will, to some degree, offset any savings. This is most likely to be significant where there is no effective commercial standards base that CCEB can exploit, forcing individual nation's defence procurement organisations to bear the full cost of standardisation (e.g. CCEB-specific data management).

5.7 Interconnection security policy

5.7.1 *The CITA must embody a practical security policy compatible with the goals of widespread interconnection between systems.*

Current security policy guidance regarding the interconnection of secure systems is still being formulated. Until an agreed policy emerges it will be impossible to decide the level of security functionality and assurance that will be necessary to support the envisaged level of interworking between CCEB nation systems.

A more fundamental difficulty exists, namely that interconnections between systems inevitably weaken security. Irrespective of security technology developments, a widely interconnected system will always provide opportunities for attack that are absent in a standalone system. Also, greater potential damage can be caused in an interconnected system by a security breach regardless of whether it was an unintentional mistake or the result of deliberate attack. A CITA will be unachievable unless the CCEB nations can strike a realistic balance between the level of security provided (and thus risk accepted) and the extent of interconnection sought.

5.8 System evolution

5.8.1 *The CITA must accept and provide for a range of standards and technologies to permit interoperability between systems of different technological vintages.*

Although the CITA will need to evolve in response to technological developments, the pace of evolution of CIS themselves will to a large degree depend upon factors outside CITA control (e.g. funding and operational constraints). This means that the CITA must support a range of compatible technologies to support continued interoperability between systems of different CITA vintages: older technologies or standards versions will need to be supported to allow a realistic period for migration. Conversely, the introduction of new technologies or standards within the CITA must not be delayed too long since this could inhibit end-systems' uptake of those technologies. A balance must therefore be struck between the desire to embrace new technological developments within the CITA and the practical ability of existing systems to evolve to maintain conformance with it.

This page is intentionally blank

6. Assessment of scope of the CITA

6.1 Introduction

6.1.1 In this chapter, the candidate services identified in Chapter 4 are assessed against criteria based on the scoping principles discussed in Chapter 5. Services satisfying the relevant criteria are considered to fall within the scope of the CITA. This chapter thus applies the third 'stage' described in Chapter 3.

6.1.2 On the basis of these criteria, certain services cannot presently be included within the scope of the CITA; there is nonetheless a likelihood that they will fall within scope at some future time. This situation arises where:

- although there is a likelihood that future requirements will emerge, no firm inter-nation requirement exists at the current time (and premature standardisation would be nugatory);

- inter-nation requirements exist but it is not considered practicable to adopt a standard at present usually because none is appropriate to warrant CCEB-wide agreement.

These cases are identified as instances where ongoing tracking by the CITA of CCEB requirements and corresponding technology developments is required.

6.2 Assessment of CITA services

6.2.1 The assessment of candidate IT services is based on the following seven key principles as defined in Chapter 4:

- **inter-nation requirement**

- **openness**

- **system boundary issues**

- **legacy issues**

- **cost/risk and procurement issues**

- **interconnection security policy**

- **system evolution**

6.2.2 All relevant assessment factors are listed for each of the candidate services in Table 6-1~~Table 6-1~~. Where the text in a particular cell is emboldened this indicates that this criterion is judged to be the primary factor determining whether the function or service is within CITA scope.

Table 6-1 Assessment of scope of the CITA

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
1: Operating system services								Not relevant.
2: User Interface Services								Largely irrelevant; remote presentation and IPC are addressed under distributed computing.
3: Network services								
Communications applications								
Messaging (including military message handling)	**There is a clear Inter-Nation requirement**	Open solutions exist for server to server message transfer protocols (i.e. X.400 P1 protocol and equivalent). The openness of mail client to server protocols (i.e. X.400 P7, POP3, proprietary mail protocols) is not clear. See note A.9	Support is only required for message transfer protocols and message content formats. The CITA does not specify messaging protocols or formats used nationally. Agreement is also required on security profiles used at boundaries, including message labeling formats.	Support is required within the messaging infrastructure for ACP127 (Radio and Teletype RATT Broadcasts) and other legacy messaging protocols.	Most COTS solutions do not satisfy all military requirements. However, systems which are designed specifically for military applications can result in higher developmental and life cycle costs due to the need to obtain additional maintenance support.	Secure message gateways may be necessary to mediate security services between domains.	COTS functionality is converging with military requirements.	Only message transfer protocols and message content formats are within CITA scope. Where attachments are to be exchanged, relevant data interchange standards also apply (see §7). Security services for messaging are considered separately below (§12)

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
3: Network services (cont.)								
Directory services	**There is a clear inter-nation requirement for an allied directory system that supports the transfer of directory information. This requires that the following are standardised (as per ACP 133):** **- access and interchange protocols;** **- common schema;** **- common security, authorisation and certificate policy.** **The directory will also be responsible for provision of security certificates which are demanded by the CCEB messaging profile.**	Standards for directory systems exist (e.g. X.500,) and have growing product support. See note A.10.	Border directory systems will be used according to national policy to ensure that sensitive national directory information is protected from the shared environment. Strong Authentication will be used for client and server connections to provide the correct levels of trust in the access and transfer of directory information.	Generally directory systems have been applied to network level services or in a localised context for local messaging systems. Support is required between an ACP 133/X.500 and either an ACP 100/ACP 117 environment or a proprietary/Internet environment. These will require integration and consolidation with ACP 133/X.500 based systems in order to scale and provide the allied service levels demanded with the full range of security requirements.	The risk to allied capability is that the directory support services are not provided in a secure and scaleable way. Since ACP 133 defines a target, nations may in the interim implement similar, yet non-interoperable subsets of the specification.	As defined in ACP 133 and other ACPs that apply directory for security services.	There is a need to rationalise and manage directory information within nations to ensure consistent information is input into any allied system.	ACP 133 must be applied to provide the most effective and secure way of providing all forms of information and voice exchange between the allied nations.
Naming and Addressing services	**There is an Inter-Nation requirement for the exchange of naming and addressing data**	Open specifications exist: DNS and X.500. Both will be required: see note A.15.	Different name services may be used internally (e.g. WINS).	No significant impact.	No significant impact.	Automated exchange of naming information may be prohibited for some interconnections.	No significant impact.	Within CITA scope.
Remote terminal services	**There is an Inter-Nation requirement for remote terminal access between nations; it is limited to legacy systems.**	IPS applications are open.	No significant impact.	Remote terminal possibly the only means of interoperability with certain legacy systems.	No significant impact.	Direct forms of interconnection, especially remote terminal, will often be precluded by security policy.	No significant impact.	Within CITA scope.
File transfer services	**There is an evident Inter-Nation requirement for file transfer.**	IPS applications are open.	No significant impact.	No significant impact.	No significant impact.	Direct forms of interconnection will often be precluded by security policy.	No significant impact.	Within CITA scope.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
3: Network services (cont.)								
ISO Services on top of the transport layer	**Inter-Nation requirements arise from:** - **those communications applications (e.g. OSIX.400 applications) that make use of specific upper layer protocols;** - **those distributed computing services that make use of, or independently provide, upper layer functionality.**							Within CITA scope. However, conformance to upper layer protocol standards is solely determined by CITA requirements in other areas (e.g. messaging, RPC). See note A.18.
Socket services								Not relevant.
4: Communications								
Networking								
Telephony	**There is a requirement to link into national telephone networks of CCEB nations during joint operations. There is also a requirement for CCEB nations to communicate over secure telephone circuits.**	Standards are available.	Secure telephony requires user equipment to conform to agreed standards, hence it is not purely a system boundary issue.	No significant impact.	No significant impact.	Secure telephony requires the use of accredited user equipment.	No significant impact.	Telephony standards are within CITA scope. Specific communications compression standards (e.g. V.42) may need to be standardised within specific nations, or for use within the CCEB communications infrastructure.
Wide area networking	**There is a requirement for standardisation of the services provided by the wide-area communications infrastructure.**	Open standards exist.	Unless interconnections are mediated by a communications application (e.g. messaging, firewall), interoperating end-systems must employ the same internetwork and transport protocol.	See system evolution.	No significant impact.	No significant impact.	Wide-area communications infrastructure evolves slowly because of the investment required for change. Wide-area networks will continue to offer services long after the corresponding standards have been superseded.	CITA scope limited to specification of the services provided by the wide-area communications infrastructure (i.e. internetworking protocols, data link and physical layer specifications at point of attachment). The technologies used to implement the service are within CITA scope, but see conclusion under Physical and non-physical bearer systems.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
4: Communications (cont.)								
Point-to-point services	**Inter-nation requirements exist.**	Open standards exist						Within CITA scope.
Tactical data link services	**Tactical data links are widely used by the CCEB nations. There is a requirement for these to be integrated into future CIS.**	De facto military standards exist.						Within CITA scope.
Network Interconnection								
Internetworkin g	**There is a requirement to standardise methods for LAN/WAN & LAN/LAN interworking for the purposes of inter-system interconnection.**	Open standards exist	Internetworking regimes used internally within a system are outside CITA scope.	No significant impact.	No significant impact.	Internetworking methods may be complicated by the need for guard or firewall mediation in interconnections.	No significant impact.	CITA scope limited to specification of the permissible modes of LAN/WAN & LAN/LAN interworking for the purposes of interconnection.
Transport services	**There is a requirement to standardise transport protocols between nations CIS**	Open standards exist	No significant impact.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	Within CITA scope.
Router services	**Inter-nation requirements exist.**	Open standards exist	Routing regimes used internally within a system are outside CITA scope.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	
Bearers								
SATCOM		De facto military standards exist.	Standardisation is only required at the boundary.					
Radio	**No Inter-Nation requirement (other than at point of attachment to wide-area communications infrastructure - see above).**	De facto military standards exist.	Standardisation is only required at the boundary.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	Within CITA scope in as far as it is necessary to capture the standards that could exist for non-physical bearer systems across the interconnection infrastructure.
Cable	**No Inter-Nation requirement (other than at point of attachment to wide-area communications infrastructure - see above).**	Open standards exist.	Standardisation is only required at the boundary.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	Within CITA scope in as far as it is necessary to capture the standards for physical bearer systems that could exist across the interconnection infrastructure.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
5: Distributed computing								
Distributed database management services								Covered under project level data management
Distributed process (RPC)	**No evidence of a present Inter-Nation requirement but future requirements may arise.**	No open standards. ONC+ RPC, DCE RPC and Windows RPC are all interoperable to an extent but not in a secure manner.	No significant impact.	No significant impact.	No significant impact.	System security policy may preclude the direct interconnection between systems demanded for RPC.	No significant impact.	Outside CITA scope at present. Possible requirements and status of standards and products need to be monitored.
Remote presentation services	**No evidence of an Inter-Nation requirement.**	Open standards exist for UNIX environment (X11). Widely licensed proprietary standards exist for the Windows environment.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	Outside CITA scope. (For other graphics services see Data Interchange above)
Distributed file services	**No evidence of an Inter-Nation requirement.**	Open standards exist (SMB, NFS).	No significant impact.	No significant impact.	No significant impact.	File services are usually at the heart of a system security policy. File sharing between systems may therefore force systems to adopt uniform security policies.	No significant impact.	Outside CITA scope. If an inter-nation requirement emerges then this service would come into scope. Security constraints would still be an issue.
Distributed time services	**No evidence of an Inter-Nation requirement.**	Open standards exist (e.g. NTP).	Different time protocols may be used internally (e.g. Microsoft proprietary).	No significant impact.	No significant impact.	System time is relevant to several system security functions (e.g. auditing) so many system security policies will preclude remote synchronisation.	No significant impact.	Outside CITA scope.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
Distributed print services	**No evidence of an Inter-Nation requirement.**	Open standards exist (SMB, LPD).	No significant impact.	No significant impact.	No significant impact.	Procedural aspects of control over printed output may limit the distribution of print jobs between systems.	No significant impact.	Outside CITA scope.
Distributed transaction processing services	**No evidence of a present Inter-Nation requirement but future requirements may arise.**	No open standards.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	Outside CITA scope at present. Possible requirements and status of standards and products need to be monitored.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
5: Distributed computing (cont.)								
Object interchange standards	**Inter-Nation requirements in this area are presently confined to the representation of objects embedded within OA documents.** **Wider use of distributed computing mechanisms for Inter-Nation interoperability is considered under the distributed computing category below.**	DCOM is to be controlled in future by an open standards body and will therefore qualify as an open standard.	Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.	No significant impact.	No significant impact.	DCOM uses RPC, for which no acceptably open security standard exists. There it will not be possible to use such mechanisms in situations where access controls need to be applied.	No significant impact.	CITA scope presently limited to OA document formats; see Document Interchange formats above.
Distributed object services (object middleware)	**No evidence of a present Inter-Nation requirement but future requirements may arise.**	Sufficiently open standards.	Competing standards are interoperable to a degree.	No significant impact.	No significant impact.	Risks associated with import of logic bombs or viruses are greatly magnified with distributed object technologies making interconnection impractical for many systems at present.	No significant impact.	Outside CITA scope at present. Possible requirements and status of standards and products need to be monitored.
Distributed system management services	**No evidence of an Inter-Nation requirement.**	No open standards.	No significant impact.	No significant impact.	No significant impact.	System management requires high access rights (e.g. Root or Administrator passwords)	No significant impact.	Outside CITA scope. (Existing standards are applicable to intra-system management of a distributed system, not for inter-system management interactions.)

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
6: Data management services								
Remote data access	**There is an Inter-Nation requirement for remote data access (e.g. between server/server environments).**	No open standards for remote data access protocols unless SQL*NET (ORACLE) regarded as dominant product. HTTP-based access protocols are widely used across the Internet; these offer limited database functionality. See note A.6.	Interworking/ middleware products exist which could offer a defined interface at system boundary but these presently offer only limited functionality.	No significant impact.	No significant impact.	Interconnection security policy will often prohibit direct client/server access between nations.	No significant impact.	Outside CITA scope for the present. Emergence of future Internet standards will need to be monitored.
CCEB level data management See note A.4.	**Interoperability requires common syntactic and semantic understanding of data. This necessitates standardisation of data definitions and schema. However, from a CITA perspective:** **- only data exchanged between systems needs to be standardised;** **- only data common to all or most nations needs to be standardised in the CITA.** **Both categories are impossible to predict fully and accurately in advance.**	Metadata standards are open but there are no open standards for military data (except geospatial and Hydrographic; see standard data products below).	For interoperability purposes standardisation can be limited to external schema. Current work presupposes a relational database-to-database method of interoperability. Object approaches providing encapsulation may permit standardisation to be limited to methods provided at system boundaries.	Much existing software uses well established military data models such as(e.g. NWTDB).	Widespread data standardisation requires huge investment. Bilateral arrangements are likely to be cheaper in some circumstances. Adoption of a CCEB-specific data model will preclude the use of many COTS products (e.g. Finance).	No significant impact.	Common data definitions obviate the need to update many local data definitions as individual systems evolve or are adapted to meet new requirements.	Within CITA scope. Unpredictability of future operations/need for flexibility to meet unforeseen interchange requirements emphasises importance of CCEB-wide rather than local agreements. However, priority for CITA data standardisation efforts should, at least initially, be on those items where there is firm evidence of a current or likely future CCEB-wide requirement for exchange of that data. CITA policy needs to recognise the possible emerging role of object-based approaches. Within CCEB the best that can at present be practically achieved is to define a common logical data model that each nation can map on to.
Nation level data management								
Data dictionary services	**Specific to individual nations, i.e. no inter-nation requirement.**							Not relevant.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
Database management system services	**Specific to individual nations, i.e. no inter-nation requirement.**							Not relevant.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
6: Data management services (cont.)								
Distributed data services								
Database replication	**There is a requirement to support database replication by 'push' only. There are some aspirations to use database replication as a mechanism to satisfy Inter-Nation interoperability requirements, although the extent of the requirement is unclear.** **Replication may be employed within individual systems to meet survivability and performance requirements - this does not justify inclusion of this service within the CITA.**	There are no acceptably open standards for replication protocols: this is the prime hindrance to standardisation. See note A.5.	It is generally not feasible to convert between replication protocols at system boundaries, so a common protocol needs to be supported by interoperating database products. This would effectively force interoperating systems to use identical products.	Many legacy systems employ flat-file databases which do not support efficient replication protocols.	Adoption of a single database product CCEB-wide will not be acceptable on procurement grounds.	No significant impact.	No significant impact.	Outside CITA scope because of openness principle.
7: Data interchange								
Document interchange standards								
Office Automation interchange formats	**There is a CCEB-wide requirement to exchange OA documents.**	MS Office formats open by virtue of market dominance. De jure document formats (e.g. ODA) are not sufficiently well supported to qualify as acceptably open. See note A.7.	Support required for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.	Many legacy OA packages in use but functionally limited converters available for many formats.	No significant impact.	No significant impact.	Concurrent support for different generations of interchange format required.	Within CITA scope.
Hypertext interchange formats	**There is a CCEB-wide requirement to exchange hypertext documents (for Intranet purposes or as an alternative interchange format for OA).** **See note A.8.**	Open formats exist (HTML plus widely supported proprietary extensions).	Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.	No significant impact.	No significant impact.	No significant impact.	Hypertext document standards are evolving rapidly but new versions are generally backwards compatible.	Within CITA scope.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
Hypertext transfer protocols	**There is a CCEB-wide requirement to transfer hypertext documents (for Intranet purposes).**	Open protocols exist (HTTP).	No significant impact.	No significant impact.	No significant impact.	HTTP only includes basic authentication. It therefore cannot be used where in situations where access controls need to be applied on the basis of subscriber identity.	No significant impact.	Within CITA scope.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
7: Data interchange (cont.)								
Business-transaction-oriented data interchange standards	**There is an Inter-Nation requirement for these interchange formats. Certain message formats (e.g. CALS) are specific to a particular business function so the strength of the CCEB-wide requirement for these is questionable.**	Effective standards (either military-specific de jure standards or open commercial specifications) exist in most areas.	Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.	Some widely-used message formats vital for continued interoperability with legacy systems.	No significant impact.	Meeting the security issues could incur significant cost and risk.	There could be significant security issues regarding the use of digital signatures with EDI.	Within CITA scope (limited to those areas where CCEB-wide requirements exist.
Military data interchange formats	**All formats identified thus far are specific to C2I systems.** **(This category does not cover formats related to message handling policy (e.g. P772) which is covered separately below.) C2I-specific messages can be included as the 'body part' of ACP 123 messages.**	These formats are military-specific but most are effective in the sense that they are widely supported.	Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.	The continuing support for the majority of these formats is required for legacy systems.	No significant impact.	No significant impact.	No significant impact.	Within CITA scope.
Character sets and alphabets	**There is a CCEB-wide requirement to support a common character set.**	International alphabet #5 (with National variants) is the only genuinely open standard at present. Future product support for internationalised character sets (e.g. UNICODE) will become more widespread. IA#5 assumed by other formats (e.g. for OA).	Support required for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	Within CITA scope.
Encoding standards	**There is an Inter-Nation requirement to exchange encoded data.**	Many open encoding standards exist.	Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	Within CITA scope.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
7: Data interchange (cont.)								
Fax standards	**There is an Inter-Nation requirement to exchange fax data.**	Open standards exist.	No significant impact.	No significant impact.	No significant impact.	Special circuits and user equipment is required for secure fax transmission.	No significant impact.	Within CITA scope. Fax transmission standards are relevant to the communications systems only.
Video conferencing standards	**There is an Inter-Nation requirement to perform video conferencing.**	Open standards exist.	No significant impact.	No significant impact.	No significant impact.	Interconnection security policy will often prohibit the direct connection required for IS-hosted video conferencing between nations (as opposed to purely comms-hosted video conferencing).	No significant impact.	Within CITA scope. Video conferencing standards are relevant to the communications systems only.
Graphical/still image data interchange standards. (geospatial data and fax formats are dealt with separately)	**There is an inter-nation requirement for standardisation for formatting digital imagery files and imagery related products.**	Many open standards exist. Some standards are military-specific, but are open in the sense that they are widely supported.	Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.	The continuing support for the majority of these formats is required for legacy systems.	No significant impact.	No significant impact.	No significant impact.	Within CITA scope.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
Geospatially referenced data interchange standards	**There is an inter-nation requirement for interchange of geospatially-referenced data (e.g. overlays). Primarily a C2I requirement.** **Formats for standard geospatial and Hydrographic data products need to be standardised across all recipient nations.**	De jure format standards exist for distribution purposes.	Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.	There are many GIS in use in existing systems and significant quantities of GIS data in proprietary formats. Legacy applications software assumes proprietary formats which will require conversion either to other proprietary formats or to less common de jure format standards. Some CITA-conformant systems will need to support additional (proprietary) formats to provide interoperability with specific legacy systems; the legacy systems themselves will dictate where and what additional formats will be needed.	Adoption of a de jure interchange format for geographically indexed data could preclude use of many COTS GIS products, unless partnership with GIS vendors helps to ensure development and maintenance of data interchange converters.	No significant impact.	No significant impact.	Formats of geospatial and Hydrographic data within CITA scope for distribution purposes. Emergence of future standards will need to be monitored and CITA extended to include overlay interchange formats.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
7: Data interchange (cont.)								
Moving image and audio/visual data interchange standards . (ITU video conferencing standards formats are dealt with separately)	**There are Inter-Nation requirements for some standards listed in this category. There is no evidence of a present Inter-Nation requirement for transfer of moving images between IS.**	Open standards exist in most areas.	Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	Within CITA scope; includes:. CD ROM (CDFS), MIME. Other areas are presently outside CITA scope. Potential future requirements for transfer of moving images between nations need to be monitored.
Audio data interchange standards (excluding ITU audio standards)	**There is evidence of an inter-nation requirement for transfer of sound between CIS.**	Open standards exist in most areas.	Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	Outside CITA scope at present. Potential future requirements need to be monitored.
File compression standards	**There is an Inter-Nation requirement to exchange compressed data.**	Many open compression standards exist.	Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.	Support may not be available on certain legacy systems for compression formats.	No significant impact.	No significant impact.	No significant impact.	Within CITA scope. The CITA should consider all open compression formats (.gz, .zip, .tar, etc.) and specify these instead of the compression utilities themselves.
Multimedia and distributed real time service data interchange standards								All standards under this category are already covered in one of the other data interchange categories. For video, see sections on Graphical/Still Image, Moving Image and Audio/Visual data interchange standards. For audio, see section on Audio Data Interchange Standards.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
Page description or display languages	**Inter-nation requirements exist for transfer of information in device-specific formats (e.g. camera-ready documents and artwork or where an application unique to one CCEB nation needs to pass a printable output to another CCEB nation's system).**	Open standards exist.	Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.	Many systems will be unable to read, display or print current page description formats.	No significant impact.	No significant impact.	No significant impact.	Within CITA scope.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
8: System and Network Management								
System management	**No evidence of an Inter-Nation requirement.** **See note A.12.**	Sufficiently open standards exist (e.g. SNMP) for cross system management.	No significant impact.	No significant impact.	No significant impact.	Security policy will usually preclude system management interactions between systems. Special considerations required for transfer of access control and authentication data between systems (see below).	No significant impact.	Outside CITA scope (no requirement).
LAN management	**No evidence of an Inter-Nation requirement for management of local area networks.** **Network management standardisation will be required within the wide-area communications infrastructure. but this is not relevant to the management of networks under the control of end-systems.** **See note A.13.**	Open standards exist for LAN management only. However, these often do not meet security requirements associated with the management of Defence systems.	No significant impact.	No significant impact.	No significant impact.	Security policy will usually preclude network management interactions between systems.	No significant impact.	LAN management is Outside CITA scope (no requirement).
National WAN management	**No inter-nation requirement (see conclusion).**							National WAN management will be managed by national staff hence there is no inter-nation requirement.
CWAN management	**An inter-nation requirement exists.** **For the immediate future, special procedures will be required to manage the CWAN.** **See note A.19.**							Within CITA scope.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
Communications bearer system management	**No inter-nation requirement (see conclusion).**							Outside of CITA scope. Communications systems will be managed by national staff hence there is no inter-nation requirement.
9: Software engineering services								Not relevant.
10: Graphics								
Graphics programming languages and APIs								Not relevant (only relevant for application and people portability).
10: Graphics (cont.)								
Application software packages having a drawing capability								Not relevant (only relevant for application and people portability)..
Military symbology standards	**Inter-nation requirements exist to pass symbolic information. This relates to the symbol types (e.g. heavy battle tank, frigate) rather than the actual graphical symbols used to represent them.**	No open standards exist, though there are military standards which are widely supported by CCEB nations.	No significant impact.	Many systems will not support adopted standards.	No significant impact.	No significant impact.	No significant impact.	The standardisation of graphical military symbols may be a desirable goal but at present it is only relevant to people or application portability. It is relevant for systems to be able to inform each other of the presence and location of other units. How those units are represented is a matter for individual nations..
11: Internationalisation								Not relevant except for character sets which are covered under data exchange.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
12a: Message Security								
Message origin authentication	**There is a clear inter-nation requirement that the origin of all formal messages can be authenticated.**	Standards exist in this area (X.509) and five nations within the CCEB have agreed common algorithms for digital signatures (e.g. DSS).	Since a digital signature is formed by encrypting a message digest or hash with a private key, common algorithms and certificate profiles are required if this is to succeed across national boundaries. The binding of the corresponding public signature key to the originator is achieved by the signing of the certificate by the Certification Authority. For certificate path processing to be successful across boundaries, the Certificate Management Infrastructure Authentication Framework also needs to extend across these boundaries.	Users on legacy systems that do not support the use of certificates and digital signatures will be unable to authenticate message origin unless a boundary device is utilised to verify the digital signature of the originator, and mechanisms are employed within the legacy system to guarantee integrity of the message between the boundary device and the recipient. Similarly outgoing messages can have the digital signature of the boundary device appended to provide a level of authentication in the other direction.	Sufficiently strong algorithms are in the public domain, and commercial products are available to implement them. Five nations within the CCEB have agreed on common algorithms for digital signatures. The main cost/risk issue is in the supporting infrastructure for the generation and distribution of certificates and tokens and the cost/risk impact of this aspect may be significant.	No further issues.	Lack of an acceptable certificate management infrastructure will slow system evolution.	The CITA should standardise authentication mechanisms in support of message transfer.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
12a: Message Security (cont.)								
Message access control	**There is a clear inter-nation requirement for exchange of clearance information and security labels in support of formal messaging.**	Standards exist in this area (e.g. X.411).	Common security policies or policy equivalence mappings are required to support this service across boundaries.	Other than communications and intelligence systems, few legacy systems support the use of security labels or the processing of clearance information.	Commercial products today do not implement X.411 with the clearance extensions hence are not regarded as providing sufficiently strong security to meet the military requirement; but they appear to be moving in this direction so the cost/risk impact may be acceptable.	No further issues.	Lack of acceptable commercial products will slow system evolution.	Within CITA scope. The current CITA should adopt: (a) X.411 security label syntax (i.e. the way the labels are represented when they are exchanged); (b) security label semantics (i.e. standardise the meaning of security labels) are currently being specified by the INFOSEC ISME For signatures, see Message Origin Authentication. However, given that, unlike NATO, the CCEB is not a treaty organisation, in the past it has been deemed impossible to take this logical step forward. (c) clearance semantics (i.e. standardise the meaning of clearance attributes) are a subset of the security label and are currently being specified by the INFOSEC ISME.
Message content privacy/confidentiality	**Three of the five CCEB nations have stated a requirement for per-message confidentiality within message transfers.**	Open standards exist for options within messaging protocols; SMIME, PCT and ACP 120 support the military requirement.	No significant impact.	Few legacy systems offer security functionality within messaging protocols.	All nations are implementing some type of security (ACP 120, PCT or SMIME) and the cost to implement the necessary mechanisms and management infrastructure for interoperability is likely to be acceptable. Different national policies on encryption may hinder adoption of a common policy.	Significant issues exist including key management and the use of common encryption algorithms.	Lack of acceptable products will slow system evolution.	Within CITA scope. The security policy should specify confidentiality options within messaging protocols.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
12a: Message Security (cont.)								
Message content integrity	**Inter-nation requirements exist for integrity options within message transfers.**	Open standards exist (e.g. SHA-1, MD5) for options within messaging protocols.	No significant impact, unless the message digest or hash is also encrypted to form a digital signature.	Few legacy systems offer security functionality within messaging protocols.	Sufficiently strong algorithms for integrity are in the public domain, and commercial products are available to implement them. However, when these are combined with encryption to form a digital signature, the main cost/risk issue is in the supporting infrastructure for the generation and distribution of certificates and tokens and the cost/risk impact of this aspect may be significant.	There are significant issues relating to the issuing and management of digital signatures and certificates as well as the adoption of common algorithms.	The reluctance of nations to decide to implement a Certificate Management Infrastructure will affect system evolution.	Within CITA scope. CITA should standardise integrity options within messaging protocols.
Certificate management and distribution	**Inter-nation requirements arise from the need to distribute signed certificates from a central issuing authority to a directory which is accessible to individual end-systems, and for individual end systems to be able to verify the authenticity of those certificates.**	There are open standards for directories (e.g. X.500) and emerging standards for Public Key Authentication Frameworks and Certificate Management Infrastructures.	There are significant boundary issues particularly in relation to directory shadowing, replication and certificate path processing.	Few legacy systems provide the necessary mechanisms.	Automated transfer of signed certificates between systems is an immature technology and represents a significant risk. Current commercial products are not deemed sufficiently secure. Alternative mechanisms such as cross-certificates are currently being examined.	There are significant issues relating to the generation, distribution, management and user validation of signed certificates.	The reluctance of nations to decide to implement a Certificate Management Infrastructure may slow system evolution.	Within CITA scope at present, but may be more realistic to be included in future CITA specifications. National policies need to be monitored to determine applicability of commercial standards and Government variants.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
Message non-repudiation with proof of origin	**Inter-nation requirements exist for non-repudiation of message transfers. No other instances of inter-nation non-repudiation requirements have been identified.**	Open standards exist (e.g. digital signatures) for options within messaging protocols.	Security policy needs to be developed to determine where the non-repudiation security service terminates.	Few legacy systems offer security functionality within messaging or other protocols, however most legacy messaging systems offer this service through procedural controls.	Commercial products implementing ACP 120 are available, and products supporting SMIME are emerging. Cost/risk issues are not expected to be significant.	Significant issues including management of digital signatures and the adoption of common algorithms.	Commercial products implementing ACP 120 are available, and products supporting SMIME are emerging.	Within CITA scope.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
12a: Message Security (cont.)								
Message non-repudiation with proof of delivery	**Inter-nation requirements exist for non-repudiation of message transfers. No other instances of inter-nation non-repudiation requirements have been identified.**	Open standards exist (e.g. signed receipts with trusted time stamps) for options within messaging protocols.	Security policy needs to be developed to determine where the non-repudiation security service terminates.	Few legacy systems offer security functionality within messaging or other protocols, however most legacy messaging systems offer this service through procedural controls.	Commercial products are available so cost/risk issues are not expected to be significant.	Significant issues including management of digital signatures and the adoption of common algorithms.	Commercial products are available.	Within CITA scope.
Message security labelling	**This is a subset of Message Access Control.**							
Message accountability	**Inter-nation requirements exist.**	Some standards do exist.	Security policy needs to be defined to determine where the accountability security service terminates.	Few legacy systems offer security functionality within messaging or other protocols, however most legacy messaging systems offer this service through procedural controls.	Implementation cost and risk will be high if commercial products cannot provide the required functionality and assurance.	Significant issues including management of digital signatures and the adoption of common algorithms.	Lack of products will affect system evolution.	Within CITA scope.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
12b: General Security								
Authentication	**There is an aspiration in future to be able to provide a CCEB-wide logon to national systems and the CWAN with automatic propagation of identity and access rights.** **Less ambitious Inter-Nation requirements include:** - **the ability to coordinate the management of user identities, access rights, passwords etc. across systems;** - **the ability to pass clearances or other privilege attributes (e.g. group memberships) between systems when making access requests.**	Open standards exist in this area (e.g. X.509), but agreement on the syntax and the semantics of clearance attributes is required.	Security properties at the boundary between systems are strongly dependent upon the mechanisms used internally so any standardisation is likely to have an extensive 'systemic' effect.	Few legacy systems offer any sophisticated security functionality which would make them amenable to interconnection in this way.	Single log-on across heterogeneous systems is an immature area which would represent a risky standardisation undertaking. A lack of commonality in approaches will be an increasingly significant impediment to interoperability. National constraints over system security policies will represent a cost and risk to many projects.	Policy may preclude access or the transmission of security attributes between systems in many cases (e.g. where the systems have different security assurance levels). Proxy servers or boundary/border devices may be the only mechanisms allowed under national security policies.	Any adopted policy that cannot be supported by commercial products will adversely affect the ability of systems to evolve.	The current CITA should standardise authentication mechanisms in support of secure inter-networking protocols.
Access control	**See authentication above.**	As with authentication, the overwhelming requirement to standardise for interoperability can be argued to outweigh the openness disadvantages. CCEB-specific standards will be required in areas such as security class labeling.	As with authentication, security properties at the boundary between systems are strongly dependent upon the mechanisms used internally. Translation of certain aspects can take place at boundaries (e.g. security classification labels).	Few legacy systems offer security functionality amenable to interconnection in this way.	Inter-Nation access control mechanisms and policies need to be established that do not force all end-systems to adopt a uniform security policy or achieve the same assurance targets.	See authentication above.	No significant impact.	The current CITA should standardise security classification labels (i.e. permissible labels and their representation). Standardisation in other areas will be conditional upon a significant shift in the market position of relevant technologies.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
12b: General Security (cont.)								
Key management and distribution	**Inter-Nation requirements arise from:** **a) the need to distribute keys from a central issuing authority to individual end-systems. This; will be determined by wider Government policy.** **b) the need for separate end-systems to exchange keys (e.g. for digital signature purposes). This is a potential CITA requirement.**	There are open standards in this area. Asymmetric keys can be distributed via PKI and Symmetric Keys can be distributed via EKMS. Nation-specific variants of open standards are under development. See note A.11.	There are several issues in both PKI (e.g. path processing across boundaries) and EKMS (e.g. common Transfer Key Encryption Keys) that need to be resolved before keys can be exchanged across national boundaries.	No significant impact.	Automated transfer of keys and other security attributes between systems is an immature technology and represents a significant risk.	Policy may preclude the transmission of security attributes between systems in many cases (e.g. where the systems have different security assurance levels or processing mechanisms).	No significant impact.	Outside CITA scope at present but may be included in medium term. National policies need to be monitored to determine applicability of commercial standards and national variants.
Confidentiality	**Inter-nation requirements exist for confidentiality and integrity options within more direct communications mechanisms, such as RPCs and transport layer protocols.**	Open standards do exist for options in transport protocols via Internet technologies (e.g. SSL, TLSP) may soon provide a solution. Operation of RPC mechanisms through firewalls is still immature.	Security policy needs to be defined to determine where the confidentiality security services terminate.	Link layer encryption has been the traditional means of providing confidentiality services, and few legacy systems offer this service at other layers. However, even if a common IP high grade crypto is achieved, it will not meet all the requirements for the foreseeable future in respect of availability, transec and traffic flow security, hence there will continue to be a need for high grade link cryptos to meet these requirements.	Inter-nation data confidentiality mechanisms and policies need to be established that do not force all end-systems to adopt a uniform security policy or achieve the same assurance targets.	At present, high grade security for connectivity can only be achieved through link layer encryption. IP based encryption is not yet sufficiently mature.	S/MIME is expected to evolve to include many of the features specified in ACP 120 and could become a suitable mechanism for application layer confidentiality services for some systems.	Scope dependent on availability of standards. Confidentiality options within direct interworking mechanisms (e.g. HTTP, RPCs) may be relevant to the medium-term.
Integrity	**See data confidentiality above.**	See above.	See above.	See above.	No significant impact.	No further issues.	No significant impact.	Scope dependent on the extent to which direct interworking services are adopted in the CITA in the medium term. As for confidentiality above.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
12b: General Security (cont.)								
Accounting and audit	**There is an inter-nation requirement.**	Open standards exist. Procedure-based mechanisms may need to be adopted.	Audit trails are usually maintained within a system boundary and require applications to produce the necessary logs. Audit logs can be passed across system boundaries (e.g. using SNMP), but national security policies may preclude this.	No significant impact.	No significant impact.	Security Operating Procedures for Accounting and Audit within nations apply. Audit logs could be passed across system boundaries, however this can weaken security (see conclusion).	No significant impact.	Within CITA scope. Accounting and audit mechanisms can be used locally to support non-repudiation Security is of concern when audit logs are passed through firewalls which typically form the boundary of a system. Management protocols (e.g. SNMP) run over UDP; operating UDP through a firewall will weaken the security it provides.
Non-repudiation	**Inter-nation requirements exist for non-repudiation of information exchange other than messaging.**	No open standards exist.	Security policy needs to be defined to determine where the non-repudiation security service terminates.	Few legacy systems offer this service other than by procedural controls.	Adoption of a non-COTS solution will increase cost and risk.	No further issues.	Any adopted policy that cannot be supported by commercial products will adversely affect the ability of systems to evolve.	Non-repudiation options within information exchange are within scope of the current CITA. However there is currently a lack of standards.
Security domain mediation	**Security domain mediation mechanisms are needed for interoperability but the requirement for them generally arises on a bilateral basis. A future CCEB security policy may give rise to a need to standardise mediation services.**	No open standards for such services presently exist. Firewall products have a general utility in securing interconnections between end-systems. However, these are not sufficiently well standardised to qualify as being open.	Firewalls typically form the boundaries of systems and are responsible for mediation between the internal system and external WAN environments.	Special enabling mechanisms will continue to be needed to mediate between the security policies of legacy systems.	Building high-assurance guard devices add to cost and risks of interconnection.	The effectiveness of a firewall is dependent upon the mediation rules that it enforces.	No significant impact.	Outside CITA scope. A future CCEB-wide security policy may bring such services within CITA scope.
13: Support application software								
OA	**There is a CCEB-wide requirement to exchange OA documents. This could be satisfied by standardising on an OA package or an interchange format.**	Dominant market leader: MS Office (at present).	Adoption of (possibly proprietary) document format for interchange sufficient for interoperability. See note A.2	Potentially relevant for some systems.	MS Office and other Windows-based products are not satisfactorily supportable in UNIX environments.	No significant impact.	Succeeding versions of OA packages provide limited backwards compatibility.	Recommending a specific OA package outside CITA scope (but see Document Interchange category above).

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
14: Collaborative Computing								
Workflow services	**There is a possible future Inter-Nation requirement for workflow services.**	Open standards are emerging.	The immature status of emerging standards make interoperability at system boundaries difficult to achieve.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	Outside CITA scope at present because there are no sufficiently open standards. Future requirements, the status of standards from the Workflow Management Coalition[16] and the status of products (e.g. Lotus Notes, SAP & PeopleSoft) need to be monitored.
On-line wide area publishing	**There is a requirement for the support of group access but in read-only mode.**	Open standards exist.	Support for designated interchange format is required at system boundaries only. Different formats may be used internally.	No significant impact	No significant impact	Write access to on-line published information would need suitable security measures in place.	Standards are evolving rapidly but new versions are generally backwards compatible.	Within CITA scope for read access only. Write access will come within the CITA scope if security issues can be resolved.
News group services	**There is a possible future Inter-Nation requirement for News group services.**	Open standards exist.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	Within CITA scope.
Whiteboarding	**There is a possible future requirement for Whiteboarding services.**	Open standards are emerging in the ITU-T T.120 series.	No significant impact.	Most legacy systems will not support Whiteboarding.	Adopting a product that subsequently fails to win market share could incur significant cost penalties.	Supporting Whiteboarding across security boundaries is likely to be prohibited because of the close coupling of user terminals and the lack of security mechanisms.	No significant impact	Outside CITA scope at present. Possible requirements and status of standards and products need to be monitored.

16 The Workflow Management Coalition, founded in August 1993, is an international organisation of workflow vendors, users, analysts and university/research groups. The Coalition's mission is to promote and develop the use of workflow through the establishment of standards for software terminology, interoperability and connectivity between workflow products. Consisting of over 130 members, spread throughout the world, the Coalition has quickly become established as the primary standards body for this rapidly expanding software market.

Section/category	Inter-Nation requirement	Openness	Boundary issues	Legacy	Cost/ risk	Interconnection Security Policy	System evolution	Conclusion
15: Special application software	**No evidence of an Inter-Nation requirement. Porting of applications may be used as a route to interoperability where no open standards exist.**	No genuinely open products.	Can avoid standardising on products by adopting interchange formats in some cases.	Potentially relevant, e.g. Nauticus.	Application standardisation may lead to undesirable procurement constraints.	No significant impact.	No significant impact.	Outside CITA scope.
GIS	**There is a requirement to share geospatial data, but no requirement to standardise on an application.**	Attempts are being made by GIS vendors to develop some standards for APIs and data interchange. Agreement by the Open GIS Consortium (OGIS) on an API standard has now been achieved.	Can avoid standardising on products by adopting interchange formats (if they ever come to fruition).	There are lots of legacy applications and geospatial data bases around.	Potentially serious implications if poor product choice is made. Some nations cannot specify a product because of procurement rules.	No significant impact	GIS data bases can be difficult to evolve or port to newer systems	Outside CITA scope. If a suitable, widely adopted data interchange format emerges then there would be no requirement to standardise on a GIS application (except of application or people portability).
Track Management	**There is a requirement to share track data (and hence a common picture), but no requirement to standardise on an application.**	There are no open standards for track management services. Military standards for passing track data exist (e.g. OTH-Gold).	Can avoid standardising on products by adopting interchange formats.	Potentially relevant. The wide use of Nauticus as the main track management application could lead to problems if support for the product changes.	Application standardisation may lead to undesirable procurement constraints	No significant impact	No significant impact	Outside CITA scope. At present interoperability can only be achieved by specification of a single product. If a suitable data interchange format emerges then there would be no requirement to standardise on a product.
Alert services	**There is evidence of an Inter-Nation requirement to pass alerts such as flash messages.** **See note A.17.**	No open standards.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	No significant impact.	Outside scope of current CITA because there are no open standards. It is deemed desirable for certain alerts to be sent between CCEB nations, particularly in relation to threat warnings. At present, however, there are no open standards and no suitable products.
Data fusion	**There is no requirement at present, however as coalition forces become more integrated there may arise a need to fuse data from disparate sources.**	No open standards.	Not applicable at present.	Not applicable at present.	Not applicable at present.	Not applicable at present.	Not applicable at present.	Outside CITA scope at present.

7. CITA Specification

7.1 Introduction

7.1.1 Table 7-2~~Table 7-2~~ summarises the recommended standards for the CITA specification (for a fuller description, including recommendations for emerging standards see annex B). This chapter is essentially a summary of stage 4 of the selection process.

7.2 Overview

7.2.1 Among the IT services that are within the scope of the current CITA, there are comparatively few technical choices available. This is because the current CITA is limited, for the most part, to those areas where technology is well-defined and standards are reasonably stable and well supported. These aspects of the profile, therefore, are unsurprising.

7.3 Key drivers

7.3.1 A key driver in the process of selecting the CITA services has been the existence (or likely existence) of user requirements and whether or not the technology exists to provide those services. The selection of standards for the CITA specification has been driven by the following:

- **adoption of Internet and web technologies.** The CITA cites the popular internetworking standards TCP, IP and UDP; the data exchange protocols in widespread use on the Internet and in commercial networks (HTTP, NNTP, FTP etc.); and common data interchange formats (HTML, JPEG, zip, etc.);

- **need for security.** The most significant departure from commercial standards is in the adoption of a common security protocol (ACP 120) particularly in support of messaging. A common approach to secure messaging is fundamental to the existence of an effective CITA;

- **adoption of essential requirements to meet military needs.** Common elements of CCEB standards for organisational messaging (ACP123) and directory (ACP133) are adopted.

7.3.2 The CITA makes no statements about the security architecture or policy to be adopted for end-systems. However, the widespread interconnection of systems envisaged means that Secure Messaging alone cannot provide adequate protection. Depending upon the protective marking of the data and/or system and the geographical location and nature of the communications bearers, messaging interconnections between systems will continue to require COMSEC

protection through the use of (an appropriate grade of) encryption at the network/link level. Even where the data exchanged has a low or even no security classification, COMPUSEC concerns, possibly derived from distant systems in the federation, will often lead to a supplementary requirement for network-level encryption.

7.4 CITA services out of scope

7.4.1 A number of CITA services are currently ruled out of scope; they are not shown in the specification summary but are listed below. Services are ruled out of scope if there is no internation requirement or there are no acceptable standards. The scope of CITA services will be kept under review by the Working Group.

Table 7-1 CITA services out of scope

No.	Service Area	Service
1.	Operating System Services	
2.	User Interface Services	
3.	Distributed Computing	Distributed process
4.		Remote presentation
5.		Distributed file services
6.		Distributed time services
7.		Distributed print services
8.		Distributed transaction processing
9.		Distributed object services (object middleware)
10.		Distributed system management
11.	Data Management Services	Data dictionary services
12.		Database management services
13.	System and Network Management	System management
14.		LAN management
15.		National WAN management
16.		Communications bearer system management
17.	Software Engineering Services	
18.	Graphics	Graphics programming languages and APIs
19.		Application software having a drawing capability
20.	Internationalisation	
21.	General Security	Security domain mediation
22.	Support Applications Software	
23.	Collaborative Computing	Workflow services
24.		Whiteboarding
25.	Special Applications Software	Geographical Information Systems
26.		Track management
27.		Alert services
28.		Data fusion

7.5 Multiple standards

7.5.1 The CITA specification generally identifies a single standard or group of interdependent standards for each service. In some cases, however, the Working Group agreed that it would be appropriate to specify multiple standards that progressively add functionality (e.g. HTML, XML & SGML). In such cases a primary standard is identified (HTML in this example) and must be supported regardless of whether any other standards are implemented.

7.6 Tabular summary

7.6.1 The set of services that are within the scope of the current CITA, the standards supporting those services and any emerging standards are summarised in the following table.

Table 7-2 Tabular summary

No.	Service Area	Service	Recommended Standard	Emerging Standards
1.	Network Services	Messaging: Organisational	Message transport submission & delivery (P1/P3/P7) ACP 123 Annex C. Gateway between MMHS and ACP127 to be defined. Content Type (P772, ACP 123 Annex A, Annex B, Annex D) Message Store Attributes (P772, MS Attributes, ACP 123 Annex E, Annex F)	
2.		Messaging: Interpersonal	SMTP (RFC 821) + MIME (RFC 2045).	
3.		Messaging: Naming and Addressing	ACP 123 (based on X.400). ACP 133 (based on X.500).	SMTP addressing schema will need to be formulated as per ACP133.
4.		Directory	ACP 133 (based on X.500 1992 with some 1997 extensions). LDAP v 3 for deployed networks	
5.		Naming and Addressing services	DNS (RFC 1034, 1035) Bind v 8.2 or higher. Internet domain naming policy. NAT (RFC 1631) for deployed networks	RAT (draft IETF standard) for deployed networks
6.		Remote Terminal services	TELNET (RFC 854/855)	
7.		File Transfer services	FTP (RFC 959) and HTTP v1.1 (RFC 2616) for file transfer - (Netscape Navigator and MS Internet Explorer and their interoperable proprietary extensions). FTP products that implement the 'Restart' elements of RFC 959 for file transfer in constrained environments.	
8.		ISO services on top of the transport layer	RFC 1006.	

No.	Service Area	Service	Recommended Standard	Emerging Standards
9.	Communications	Telephony	**Secure telephony:** STU-IIB compliant equipment. **Insecure telephony:** Standards selected from ITU-T Recommendations: Series E; Series G; Series P; Series Q; Series V. V.34 for modems. V.42 for communications compression	STE (Secure Telephone Equipment). Voice-over-IP standards. V.90 modem standard (56 Kbits/sec).
10.		Wide area networks	Internetworking - IPv4 (RFC 791). X.25 + X121 Addressing policy. ISDN - ITU-T I. series of standards. B-ISDN (ATM) - ITU-T I. series of standards + ATM Forum af-standards for physical and adaption layers and LANE v 2.0. SONET/SDH - ANSI T1.105. X.121 addressing policy.	
11.		Point-to-Point services	RFC 1661/1662 (PPP) RFC 1332 (PPP Internet Protocol Control Protocol (IPCP)) RFC 1989 (PPP Link Quality Monitoring) RFC 1994 (PPP Challenge Handshake Authentication Protocol (CHAP)) RFC 1570 (Link Control Protocol (LCP) Extensions).	
12.	Communications (cont.)	Tactical Data Link services	**Link 11** STANAG 5511 annex B, Radio performance & protocols; vol.2, Link 11B Waveform protocol changes. MIL-STD-118-2031a, Conventional Link 11 Waveform 16 tones. SPAWAR-5-850, Single tone Link 11 Waveform. **Link 16** STANAG 4175 edition 1. **Link 22** UHF: STANAG 4372 (Saturn); Saturn can also carry Link 11 and Link 16 messages. HF: STANAG 4444 (Slow hop ECCM). **Link forwarding:** STANAG 5616.	VMF.
13.		Internetworking Standards	IP v4 (RFC 791) and the following associated standards: IP Sub-netting (RFC 950) Broadcasting Internet Datagrams (RFC 919) Broadcasting Internet Datagrams in the presence of subnets (RFC 922) Internet Control Message Protocol (ICMP) (RFC 792) Awaiting CCEB policy on IP addressing. DHCP (RFC 2131) for deployed networks	IPv6 (RFC 1883).
14.		Transport services	TCP (RFC 793) UDP (RFC 768).	

15.		Routers	RFC 1812 - Requirements for IP Version 4 Routers BGP - 4 (RFC 1771) OSPF v2 (RFC 2328)	

No.	Service Area	Service	Recommended Standard	Emerging Standards
16.	Communications (cont.)	SATCOM bearers	**General** MIL-STD-188-146 Interoperability And Performance Standards For Satellite Communications, 15 June 1998. **UHF** MIL-STD-188-181A, Interoperability Standard for Single Access 5-kHz and 25-kHz UHF Satellite Communications Channels, 31 March 1997. MIL-STD-188-182A, Interoperability Standard for 5-kHz UHF DAMA Terminal Waveform, 31 March 1997. MIL-STD-188-183, Interoperability Standard for 25-kHz UHF/TDMA/DAMA Terminal Waveform, 18 September 1992; with Notice of Change 1, 2 December 1996 (STANAG 4231). MIL-STD-188-184, Interoperability and Performance Standard for the Data Control Waveform, 20 August 1993. MIL-STD-188-185, DoD Interface Standard, Interoperability of UHF MILSATCOM DAMA Control System, 29 May 1996. **SHF** MIL-STD-188-164, Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, 13 January 1995. MIL-STD-188-165, Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), 13 January 1995. **EHF** MIL-STD-1582D, EHF LDR (Low Data Rate) Uplinks and Downlinks, 30 September 1996; with Notice of Change 1, 14 February 1997 (STANAG 4233). MIL-STD-188-136, EHF MDR (Medium Data Rate) Uplinks and Downlinks, 26 August 1995; with Notice of Change 1, 15 August 1996, and Notice of Change 2, 14 February 1997 (STANAG 4522).	

No.	Service Area	Service	Recommended Standard	Emerging Standards
17.	Communications (cont.)	Radio bearers	**LF/VLF** MIL STD 188-140A, Equipment Technical Design Standards for Common Long Haul/Tactical Radio Communications in the LF Band and Lower Frequency Bands, 1 May 1990. **HF** MIL STD 188-141A , Interoperability and Performance Standards for Medium and High Frequency Radio Equipment Standard. STANAG 4203 Technical standard for single channel HF radio equipment. **VHF** MIL STD 188-242, Tactical Single Channel (VHF) Radio Equipment. STANAG 4204 Technical standard for single channel VHF radio equipment. **UHF** MIL STD 188-243, Tactical Single Channel (UHF) Radio Communications. STANAG 4205 Technical standard for single channel UHF radio equipment. **SHF** MIL STD 188-145, Digital Line-of-Sight (LOS) Microwave Radio Equipment. **CNR (Voice only)** CNRs are only interoperable for fixed frequency (VHF) voice communications only. There are no commonly agreed standards for frequency agility. The standards are: QSTAG 734 (STANAG 4204) Technical Standards for Single Channel VHF Radio Equipment. QSTAG 1108 (STANAG 4197A) Common Critical Crypto Standards for Single Channel Communications (Voice, Teletype and Data) for VHF CNR. **Data modems** MIL-STD-188-110A Interoperability and Performance Standards for Data Modems. STANAG 4285 Characteristics of single tone modems for HF radio.	**CNR -** Joint Tactical Radio (JTR).
18.	Communications (cont.)	Cable bearers	RS-232, RS-422, RS-423, RS-530; EIA - 4920000-A; EIA - 5090000. Other standards covered under wide area networks.	
19.	Distributed Computing	Distributed database management services	(See under Nation-level Data Management).	
20.		Object Interchange services	CORBA/IIOP v 2.4; DCOM.	
21.	Data Management	Remote data access	ODBC v 3 (ISO 9075-3)	JDBC; HTTP-based protocols.
22.		CCEB level data management	Standards yet to be defined. Data definitions should focus on those data items for which there is an inter-nation exchange requirement.	
23.	Data Interchange	Business-transaction-oriented data interchange standards	STEP/ISO 10303 for product data; UN/EDIFACT/ISO 9735 for EDI.	XML

24.	Military data interchange standards	STANAG 5511 (Link 11 standard); STANAG 5516 (Link 16 standard); STANAG 5522 (Link 22 standard); OTHT-Gold; ADatP3 (STANAG 5500).	VMF.

No.	Service Area	Service	Recommended Standard	Emerging Standards
25.		Office Automation interchange formats	**Primary Standard** MS Office 97 interchange formats preferred. **Secondary Standard(s)** Rich Text Format (RTF) for documents if MS Office 97 format not available. Portable Document Format (PDF). Ascii (TXT) for constrained environments	MS Office 2000 interchange formats replacing MS Office 97 interchange formats as the primary standard.
26.		Hypertext interchange formats	**Primary Standard** HTMLv4.01 (Dynamic HTML). **Secondary Standard(s)** SGML for high value, complex publications; XML 1.0 where meta-language data definitions are required. WML for constrained environments.	XML replacing HTML as primary standard as is XHTML v 1.0
27.		Hypertext transfer protocols	HTTP v1.1 (RFC 2616). HTTP with Distribution and Replication Protocol for use in constrained environments.	HTTP V 2.0.
28.	Data Interchange (cont.)	Character sets and alphabets	International Alphabet 5 (ASCII). 8 bit byte code ISO 8859-1	
29.		Encoding standards	**Data Encoding Standards:** UUENCODE; MIME; SMIME; zip. **Voice encoding standards:** A-law and µ-law (ITU-T G.711). CELP.	
30.		Fax	**Secure fax:** STU-IIB compliant equipment (STANAG 5000 / MIL-STD-188-161D). **Insecure fax:** Group 3 & Group 4.	**Secure fax:** STE.
31.		Video conferencing	ITU-T H.320, ITU-T H.221, ITU-T H.224, ITU-T H.242, ITU-T H.261, ITU-T H.230, ITU-T H.231, ITU-T H.243, ITU-T H.233, ITU-T H.234, ITU-T H.244.	ITU-T H.323 with ITU-T T.120
32.		Graphical/still image data interchange standards.	JPEG File Interchange Format v1.02; GIF Version 89a, July 1990; PNG. National Imagery Transmission Format Standard NITFS 2.1 (MIL-STD 2500B/ STANAG 4545)	BIIF (ISO 12087 pt. 5)
33.		Geospatially referenced data interchange standards	DIGEST v 2; S-57 edition 3.	
34.		Moving image and audio/visual data interchange standards.	CDFS (ISO 9660); PCM for audio (ISO 11172-3); MPEG2 (video).	ITU-T H.323 with ITU-T T.120
35.		Audio data interchange standards	PCM (ISO 11172-3).	
36.		File compression standards	zip.	

37.		Page description	**Primary Standard** PostScript (Level I and II); EPS. **Secondary Standard(s)** PDF.	
38.	System & Network Management	CWAN	Procedures defined by Quad C.	

No.	Service Area	Service	Recommended Standard	Emerging Standards
39.	Graphics	Military symbology standards	MIL-STD-2525B (Symbol codes only).	
40.	Message Security Services	Message origin authentication	ACP 120 (based on X.509 authentication framework).	
41.		Message access control	Syntax of security label currently being prepared by the CMI WG of the INFOSEC ISME.	
42.		Message content privacy/confidentiality	Based on X.509 authentication framework.	
43.		Message content integrity	ACP 120.(based on X.509 authentication framework).	
44.		Certificate management and distribution	X.500 and ACP 120.(based on CMI X.509 authentication framework).	
45.		Message non-repudiation with proof of origin	ACP 120 (based on digital signatures within the CMI Authentication Framework and associated PKI).	
46.		Message non-repudiation with proof of delivery	ACP 120 (based on digital signatures within the CMI Authentication Framework and associated PKI).	
47.		Message accountability	ACP 120 (based on digitally signed receipts and PKI).	
48.	General Security	Authentication	X.509 - Awaiting CCEB policy.	
49.		Access control	Awaiting CCEB policy.	
50.		Key management and distribution	Awaiting CCEB policy.	
51.		Data confidentiality	ACP 120 application layer data confidentiality or link level encryption.	
52.		Data integrity	ACP 120 application layer data confidentiality or link level encryption.	
53.	Collaborative Computing	On line wide-area publishing services.	**Primary Standard** HTTPv1.1 (RFC 2616)/HTMLv4.01. **Secondary Standard(s)** SGML (ISO 8879) for high value, complex publications; XML 1.0 where meta-language data definitions are required.	
54.		News Group services	NNTP (RFC 977).	

8. Applicability and compliance

8.1 Introduction

8.1.1 This chapter describes the applicability and compliance aspects of the CITA. The scope of the CITA's applicability is defined in terms of the various people or groups as well as the range of systems that will benefit from it. Compliance with the CITA is defined by a number of levels which reflect the level of interoperability required by the end users.

8.2 Scope of CITA applicability

8.2.1 The scope of the CITA applicability extends from the coalition of CCEB nations to groups within individual CCEB nations, namely the end users, the project sponsor, the project manager and the system supplier.

- the *CCEB coalition* benefits from the improved operational effectiveness that could be achieved by a federation of interoperating systems using the services and standards defined by the CITA;

- the *end user* benefits from improved access to information and improved information exchange capability;

- the *project sponsor* benefits from an improved focus on interoperability requirements, an understanding of readily realisable services, the ability to re-use existing interoperability requirements and the standards that support them;

- the *project manager* benefits from improved effectiveness of procurement, clearer management of risk, reduction in cost and faster acquisition;

- the *system supplier* benefits from a clearer understanding of the customer's interoperability requirements and better stability of those requirements.

8.3 Applicability to systems

8.3.1 The CITA is applicable to national CIS that are required to participate in a CCEB-wide CIS federation, exchanging information across national boundaries and between CCEB nation forces during combined operations. Clearly, not every participating CIS will implement the whole of the CITA because the national operational requirements of the CIS are unlikely to need all the services addressed by the CITA.

8.3.2 The extent to which a particular system implements the services defined within the CITA determines its scope for interoperability with other CITA-compliant systems. A fundamental principle of CITA compliance is that where a CIS offers a service for interworking across CCEB nations, that service will be implemented according to the CITA specification. However, there will be different levels of CITA compliance according to the actual services involved.

8.4 Compliance levels

8.4.1 CITA compliance is defined by the level of interoperability a system is required to support or is capable of supporting. CIS vary significantly in their complexity and the functionality they support; they should, therefore, implement only those services that they require or can supply.

8.4.2 The interoperability levels are defined as a progressive scale of CIS functionality with identified points on the scale corresponding to common system capabilities. Thus, the lowest levels of the scale applies to systems offering basic interconnection and simple data exchange, while the upper end of the scale describes sophisticated systems with full network interconnection and able to transact complex data objects across the CIS federation.

8.4.3 The set of interoperability levels are as follows:

Table 8-1 Compliance levels

Interoperability. Level	Name	Description
1a	Basic document exchange	OA document interchange, hypertext, character sets/alphabets, graphics/still and moving images, file compression, page description, security labeling, accounting and audit.
1b	Full document exchange	As for 1a plus military transfer formats, military symbols (codes only) and standard data products.

Interoperability. Level	Name	Description
2a	Network connection	Inter-networking, transport and domain name services.
2b	Basic Intranet connection	File transfer and interpersonal email with attachments[17].
2c	Web connection	Hypertext transfer, on-line publishing and news group services. Security labeling syntax, semantics and positioning within published documents. Also web authentication and access control mechanisms.
2d	Organisational messaging	Organisational messaging based on X.400 as defined in ACP 123. Also messaging security services.
2e	Directory services	Directory services based on X.500 as defined in ACP 133.
3a	Secure database access/exchange	Database management, remote database access, data dictionary, CCEB data model and associated security services.
3b	Distributed applications	Distributed computing, object interfaces and object middleware if relevant. Also database to database replication, collaborative computing and special applications.

8.4.4 Level 1 compliant systems can read and write files in the formats cited; transfer is either manual (e.g. floppy disk) or through dedicated links.

8.4.5 Level 2 compliant systems should be able to connect to a CCEB Intranet and perform web access, email, and formal messaging. Level 1 and 2 together broadly equate to NATO level 4 interconnection.

8.4.6 Level 3 compliance is not fully satisfied by the current CITA specification but may fall within the emerging CITA. Level 1, 2 and 3 together broadly equate to NATO level 5 interconnection.

17 The CCEB requirement for interpersonal email has recently been agreed.

8.4.7 A statement showing the level of compliance with the CITA will be required for every participating national CIS, so that its scope for interoperability within the CCEB federation becomes apparent. Nations must assume responsibility for carrying out compliance checks on their own systems and issuing compliance statements to the CITA WG. Ideally, compliance with at least one of the defined CITA levels should be mandatory but allowance will have to be made for possible exceptional factors until experience with CITA systems has been gained.

9. CITA evolution

9.1 Introduction

9.1.1 This chapter describes the way the CITA will evolve in future issues of ACP 140. It identifies the key change drivers that affect the functionality of CIS and the technology supporting them.

9.2 Change Drivers

9.2.1 The evolution of the CITA will be driven by the following key factors:

- new technology and its uptake in the market place;
- new requirements from the stakeholders, other nation-specific interoperability technical architectures and single service forums (e.g. ABCA);
- resolution of shortfalls in long-term technical issues;
- feedback from projects implementing the CITA, external stakeholders and relevant bodies.

9.3 New technology developments

9.3.1 Close monitoring is required of the following technology areas to identify if and when acceptably open, capable standards suitable for CCEB use become available:

- HTTP-based remote data access protocols and its potential for providing a solution to the problem of shared databases;
- executable content (e.g. Java applets) in hypertext documents and associated content-specific hypertext transfer protocols ;
- internationalised character sets, in particular the move from 8 bit to 16 bit character sets;
- automatic directory shadowing/chaining protocols;

- security services within direct interworking mechanisms (i.e. other than in messaging)[18];

- distributed audit mechanisms;

- security domain mediation[19].

9.3.2 **GIS interchange standards.** The market uptake of NATO DIGEST as an interchange standard by mainstream COTS GIS vendors should be tracked. In order to succeed as a standard, and provide a credible interoperability service it must be supported by the vendors. The vendor-led developments within the Open GIS consortium include the definition of product service standards and data interchange standards. These should also be tracked as they potentially provide a powerful mechanism for map, chart and overlay exchange.

9.3.3 **Security framework and interconnection policy.** Fundamentally important to the above technology areas are the security services for the full range of direct interworking mechanisms. They are relevant to both the inclusion of more sophisticated forms of interworking in the CITA (e.g. distributed object services, RPC), and also to how widely and effectively more basic interworking mechanisms can be employed (e.g. hypertext transfer, file transfer). The CCEB aspiration for a highly interconnected federation of interoperating CIS will be severely limited unless appropriate security policies are widely implemented. ACP 120 is developing a common security protocol to support X.400 messaging. However, the scope of ACP 120 will need to be considerably expanded to provide the full range of security services needed to support direct interworking between CCEB CIS. Without such agreement, system interconnections (other than those where messaging alone is employed) will require ad hoc agreements and solutions that may be costly to reverse. Monitoring will not be sufficient; work is needed to determine whether enhancements or modifications to commercial technology and practices will be necessary to allow their application.

9.4 New CCEB requirements

9.4.1 As technological developments impact upon the way CCEB nations perform combined operations, there is an increasing need to monitor new and changing requirements relevant to the CCEB coalition. The assessment indicates that the CITA should monitor a number of service areas for possible inclusion in future CITA specifications. These additional services would enhance the capabilities of the existing CITA by:

---

18 Authentication, access control, data confidentiality, data integrity and non-repudiation services.

19 For example, adequately assured firewalls and guards.

a) overcoming some significant information exchange limitations arising from a lack of acceptably open standards (e.g. Collaborative Computing services);

b) providing CCEB-wide coherence of security and interconnection policies and the associated security services needed to allow the widest possible use to be made of existing interoperability services (e.g. http). This would allow over-restrictive security constraints limiting information access to be relaxed;

c) standardising more advanced interoperability mechanisms such as RPCs, other distributed computing mechanisms and database replication services (see 9.4.2); these are also contingent on the security developments above;

d) accommodating emerging requirements for the exchange of multimedia-based services between nations.

9.4.2 There are already various aspirations within CCEB for the use of database replication as an interoperability mechanism; unfortunately, an open solution is not feasible, nor can any existing proprietary solution meet all CCEB requirements. Monitoring is needed here to determine whether the scale of the requirement grows to the point where adoption of a proprietary solution is justified.

9.5 Resolution of shortfalls in long term technical issues

9.5.1 There are several key areas where firm CCEB technical policy is needed for the emerging CITA, but where shortfalls are evident. Resolution of some shortfalls is fundamental to achievement of CITA interoperability aspirations; the shortfalls described here, however, are not fundamental impediments to interoperability, but will limit effectiveness and cost-efficiency.

9.5.2 **Message handling.** Messaging policy has been developed within the CCEB under the direction of the (now dissolved) AIS ISME, but shortfalls in regard to the CITA remain. The number of vendors who provide X.400 products that support the facilities required for military messaging is extremely small. The lack of policy on inter-personal messaging has now been resolved and SMTP email adopted as the standard.

9.5.3 **Messaging security.** The policy across the CCEB nations is being developed by the INFOSEC ISME. The impact of security on the overall architecture of the message handling backbone and of the attached end systems is still being defined. For interoperability to be achieved it is imperative that this work progresses quickly to a successful conclusion. A proliferation of Red Gateways would be undesirable, hence the completion and ratification of ACP 120 is essential. Also, now that SMTP has been adopted for interpersonal messaging, it must be included within ACP 120 along with X.400 messaging.

9.5.4 **Representation of security class label**. CCEB-specific security class label syntax and semantics must be specified to support secure messaging and possibly other forms of secure interworking envisaged for the CITA.

9.5.5 **CCEB level data management.** In order to transfer meaning and context of data successfully between systems, agreement is needed on:

- data schema (i.e. the entities and attributes present in a model and the relationships between them);
- data syntax (i.e. the permissible values of the attributes, and the concrete representation of those values);
- data semantics (i.e. the meaning of attributes and interpretation of the values within the context of the data schema).

9.5.6 As a bare minimum there needs to be an agreed model of essential data items so that individual nations can map between their internal models and this centrally agreed model. Where any elements of the data model are not defined on a CCEB-wide basis, supplementary local agreements will be required, at least in the interim. The shortfall is that no agreed data model currently exists nor does any policy for its use.

9.5.7 In the absence of an agreed CCEB-wide data model, nations will agree bilateral data interchange conventions. These local agreements will be costly to maintain as systems evolve, will require reconciliation whenever new interchange requirements are identified, and will eventually become so entrenched that re-orientation of systems to a CCEB standard will be increasingly impractical. Data definition activity is therefore required in the near-term in order to reduce the longer term impact of the current absence of a comprehensive corporate data model. From a CITA perspective, this activity should focus on those data items for which there is firm evidence of an existing or likely inter-nation exchange requirement. These agreements should be maintained in a central repository to provide a baseline for formulating more widespread agreement and for de-confliction.

9.5.8 **Name and address allocation.** The CITA Working Group was unable to ascertain who is responsible for CCEB policy on IP addressing and Internet domain names allocation. An optimal IP addressing plan cannot be defined until other policies, specifically that relating to a backbone IP network, are defined. Addressing policy is not a high priority for the present because of the limited degree to which individual systems will share communications networks or employ direct internetworking mechanisms. A viable policy will, however, be vital to achievement of CITA objectives as more sophisticated interworking mechanisms are employed.

9.5.9 **NT Domain-name policy**. In addition to the above, the expected increase in the scale of use of Windows NT-based networks throughout CCEB will demand a CCEB policy for the consistent naming of NT domains. Such a policy does not apparently exist. A similar approach to that adopted for IP addressing could be followed in which CCEB assumes responsibility for

defining the top-level policy and national authorities for defining their own nation boundaries and allocating names within their nations. In the longer term it is anticipated that Windows 2000 will replace Windows NT. In this event the need for a separate domain naming policy will diminish as Windows 2000 domains follow the DNS hierarchy.

9.5.10 **Coalition wide-area networking (CWAN)**. System interconnections have, in general, been achieved by bilateral agreement, often using dedicated point-to-point capacity rather than wide area switched data networks. Some national systems implement IP routed networks locally but few, if any, are interconnected with systems from other CCEB nations. This is generally because it is not permitted on security grounds or is not feasible technically[20]. Implementation of a coherent coalition-wide network (e.g. as demonstrated at JWID), coupled with appropriate security and technical policies, would deliver cost savings and efficiency gains. In order to achieve a single backbone IP data networks it will be necessary to define and implement a number of related technical policies, such as an overall security framework and interconnection policy (see above), naming and addressing policies for Internet domain names and IP addresses, and a coherent pan-network routing policy.

9.5.11 **CWAN Management.** In any federation of systems and networks, the management functions are normally performed by a wide range of individuals, activities and organisations. In the CWAN environment these functions are performed by a coalition communications control centre known as the Quad C. The role of the CWAN is described in section A.19.

9.6 Feedback from projects and external stakeholders

9.6.1 As ACP 140 starts to become widely published and used, there will inevitably be feedback from projects and other stakeholders. System designers and integrators will be able to contribute positively to the knowledge embodied within the CITA, thus increasing its usefulness and relevance. They will also be able to test the dependencies between the technical architecture, embodied in the CITA, and the systems and information architectures as they are instantiated in delivered systems.

9.6.2 Work carried out under the auspices of the CCEB is frequently used by and influences other nations and coalitions such as NATO. It is anticipated, therefore, that as other groups formulate technical strategies for achieving system interoperability, there will be additional feedback into the CITA Working Group.

[20] For example, if they use incompatible naming, addressing or routing policies.

10. Management

10.1 Introduction

10.1.1 The CITA, as has been shown, represent the current CCEB coalition view of the services required to support interoperability and the most appropriate (recommended) standards that should be adopted in providing those services. It is also recognised that key drivers in the specification of the CITA are rapidly changing and the CITA must keep pace with significant developments. It is essential, therefore that change is managed appropriately. This chapter discusses the management issues that will govern the way ahead for the CITA.

10.2 Development of CITA management framework

10.2.1 The work thus far has focused on the technical definition of the CITA. A management framework is needed to maintain, evolve and apply the CITA. A number of key management issues have been noted. These are briefly discussed here.

- technical management of the CITA;
- CITA implementation strategy;
- coordination between national technical architectures.

10.3 Technical management activities associated with the CITA

10.3.1 The scope of the CITA outlined above indicates that a number of management activities are required to maintain and apply CITA policies to CCEB CIS. These include:

- *Technical policy formulation.* This is the process of deciding, maintaining and ensuring conformance with technical policy for those services that fall within CITA scope. For the most part this means selection of technical standards but in some cases may require appraisal and selection of specific products (subject to legality) to represent CITA standards. For those areas currently outside CITA scope but having future potential, this activity also includes monitoring of relevant technical developments.

- *Security policy formulation.* This is the process of defining coherent security policies for the federation of CCEB CIS, a necessary precursor to the definition of specific security measures required for any given system interconnection. This is also necessary in order to be able to specify technical

policies for CITA security services. INFOSEC staffs, and individual nation's security authorities will need to undertake formulation of relevant policies.

- *CCEB directory administration*. This includes definition of the CCEB Directory schema and management of the compilation and maintenance of a CCEB-wide directory (either through central maintenance or top-level management of registrations). This is included in ACP 133

- *Data management*. This includes identification of the CCEB metadata standards and associated procedures, plus maintenance of a CCEB-wide Data Model. Specific activities will include resolution of data definition conflicts. Responsibility for these activities falls to the appropriate national data management authorities.

- *Naming and addressing management*. This includes the definition of naming and addressing policy and allocation of:
  - Internet domain names;
  - IP network addresses.

10.4 CITA implementation strategy.

10.4.1 To date, the emphasis of CITA work has been on developing a suitable technical specification. However, the objectives of the CITA will only be realised if the specification is widely followed. A CITA implementation strategy needs to be developed covering the following:

- a work plan for resolution of relevant technical policy shortfalls;
- a conformance policy for new CIS;
- a migration policy for legacy CIS;
- a detailed implementation programme;
- change management and version control processes.

10.5 Coordination between nations

10.5.1 The work carried out by the CITA WG has identified that the participating nations have differing (though broadly similar and compatible) views of the architectures (technical, system, information, business etc.) that are required to build systems. Also, the nations are all at different stages in their architecture definition and development. Each nation's development is subject to differing evolutionary pressures and are, therefore, formulating their own technical policies. Additionally, the CITA will expand in scope to embrace new IT services, changing requirements, new requirements, and evolving technology.

10.5.2 In order to manage these developments effectively there should be a CCEB-wide *coordinating* focus for CITA technical policy formulation. Strong coordination will be essential to ensure national initiatives remain sufficiently well aligned to support interoperability.

10.5.3 Furthermore, responsibility for the CITA technical policies could be delegated to various groups within the constituent nations. Nation-specific or other more local policies are likely to form the starting points for identifying CITA standards (as has happened with the US JTA and UK DTA forming the primary inputs to the CITA). Thus to ensure satisfactory management, close liaison will be required with relevant national technical authorities.

This page is intentionally blank

11. Summary and Recommendations

11.1 Introduction

11.1.1 This chapter summarises the scope of the CITA and the consequent recommendations of the CITA Working Group.

11.2 Summary of the CITA scope

11.2.1 A number of strategic principles have been identified that influence the technical scope of the CITA. When these principles are applied, the scope of a CITA for the near term equates to those standards required for a CCEB 'Intranet'. It includes those services in widespread use on the Internet (and also in individual commercial Intranets) together with a small set of additional security services essential for CCEB CIS interworking. This set of services will support a highly effective federation of interoperating systems.

11.2.2 The emerging CITA identifies extensions which will achieve the higher level of interconnection (i.e. level 5) set as the goal by the CCEB EG, and will reduce the need for supplementary bilateral agreements.

11.3 Achievements and benefits of the CITA

11.3.1 The work carried out thus far has achieved the definition of a technical architecture that is implementable now, and has the capability of supporting a highly effective federation of interoperating systems. It has also identified the services that, although out of scope at present, are likely to come into scope in the foreseeable future and will serve to increase the combined capability of the CCEB nation's CIS.

11.4 General issues raised by the CITA

11.4.1 **Specification of products.** In a number of cases, particularly where de facto standards have been adopted, the pursuit of interoperability would be facilitated by the specification of individual products (e.g. for office automation or database replication). Some nations are quite at liberty within the confines of their national law to specify individual products without risk of legal action from excluded vendors. Other nations are specifically prohibited by their national law from making such pronouncements. The CITA has, therefore avoided the specification of individual products; instead it has opted to identify, where necessary, information representation

standards, which, although developed by a single vendor, are supported by several vendors (e.g. MS Office format is supported by a number of OA vendors).

11.4.2 **Use of standards.** The role of standards in a technical architecture has many clear advantages, however it must be realised that the use of standards does not guarantee that systems will interoperate. The use of standards provides the foundation on which interoperable systems can be built. It is still necessary for end systems (and users) to have a common understanding of (i.e. attach the same meaning to) the information that is exchanged.

11.4.3 **Lack of mandated requirements.** There is no endorsed or mandated CCEB interoperability requirements or overall CIS architecture. As a result the CITA specifies the standards that should be adopted for the interworking services within its scope but does not identify a minimum set of interworking services which must be supported by all CCEB nation's CIS. Initiatives to develop these will affect the future development of the CITA and, in particular, those outlined in the rest of this chapter.

11.5 Resolution of critical CCEB technical policy shortfalls

11.5.1 A CITA is feasible subject to resolution of some technical policy shortfalls. There are three areas relevant to the current CITA specification where critical shortfalls in CCEB technical policy are evident. These are primarily:

- Message handling and message security policy with respect to the use of SMTP for interpersonal messaging;
- Representation of security class labels in support of messaging and other forms of secure interworking;
- CCEB level data management to ensure correct transfer of the meaning and context of data successfully between systems;
- Name and address allocation on IP addressing and Internet domain names allocation.

11.6 Emerging areas for CITA

11.6.1 The emerging CITA encompasses various services not present in the current CITA. Specific standards have been recommended for some of these services, but for many others no standard has been put forward. These standards gaps are an inevitable consequence of the emerging CITA's more aspirational nature. Each gap in the emerging CITA can be attributed to one or more of the following:

- a CCEB requirement could emerge within the timescales of the emerging CITA, but the precise nature and eventual scale of that requirement are not yet certain. The appropriateness of adopting a CITA standard, and the specific standard itself, thus cannot be fully ascertained at this time;

- technology is developing and associated standards are emerging but they remain immature or are not yet well supported. Standards selection must therefore be deferred until commercial trends are clearer;

- there are shortfalls in technical policy such that selection of a standard is either not yet possible or undesirable at this time (e.g. premature selection might attract significant cost and risk).

- the inability, on legal grounds, to specify individual products means that where no standards are acceptably open or widely supported (e.g. GIS) the CITA must remain silent.

11.7 Recommendations

11.7.1 It is recommended that the specification in chapter 7 is adopted as issue 1.0 of the CITA.

11.7.2 It is recommended that appropriate action taken with regard to the policy shortfalls identified in this report. Suitable policy needs to be developed in timescales commensurate with nation's needs. For those CITA services where there is no present policy an appropriate CCEB group should be identified and tasked as a matter of urgency. Specifically the following remedial actions are recommended:

- technical policies should be formulated for security services beyond those required for X.400 messaging promulgated in ACP 120. This is required to support inter-nation interoperability, including the need to support the more sophisticated interoperability mechanisms envisaged for the emerging CITA;

- data standardisation activities should be targeted directly towards data definition where there are existing or likely inter-nation exchange requirements. This must be undertaken in timescales compatible with near-term needs;

- a CCEB body should be tasked with formulating Domain Naming and IP addressing policy;

11.7.3 In addition, there is a need to monitor a number of areas for possible inclusion in the emerging CITA. These services have been excluded from the scope of the current CITA on the grounds that either no firm inter-nation requirement exists at the current time or an inter-nation

requirement exists but it is not considered practicable to adopt a standard at present. These additional services would enhance the capabilities of the emerging CITA by extending the range of interworking mechanisms available, by supporting a broader range of information exchange formats and standards, and by providing the underpinning security framework and services needed to exploit these fully. Specifically the following developments should be monitored:

- the direction of the commercial GIS market should be monitored for vendor initiatives and emerging standards for geospatially referenced data interchange standards;

- the growing use of HTTP-based protocols for remote database access and the transfer of executable contents (e.g. Java applets) in hypertext documents should be monitored.

12. Acknowledgments

The CITA Working Group is grateful to all the CCEB Nations staff, and other CCEB working groups who contributed to this document.

This page is intentionally blank

13. List of abbreviations

ACP	Allied Communications Publications
ADatP3	Allied Data Publication (Volume) 3
API	Applications Program(ming) Interface
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation.1
C2I	Command, Control and Intelligence
CAD	Computer-aided Design
CALS	Computer-aided Logistic Support
CAM	Computer-aided Manufacture
CASE	Computer-aided Software Engineering
CASM	CESG Architecture for Secure Messaging
CCE	Common Communications Environment
CCEB	Combined Communications and Electronics Board
CD-ROM	Compact Disk Read Only Memory
CDFS	Compact Disk File System
CESG	Communication Electronic Support Group
CIDR	Classless Inter-Domain Routing
CIS	Communication and Information Systems
CITA	Combined Interoperability Technical Architecture
COE	Common Operating Environment
COMPUSEC	Computer Security

COTS	Commercial Off The Shelf
CWAN	Coalition Wide Area Network
DAP	Directory Access Protocol
DBMS	Database Management System
DCE	Distributed Computing Environment
DCOM	Distributed Component Object Model
DDE	Dynamic Data Exchange
DHCP	Dynamic Host Configuration Protocol
DIE	Defence Interoperability Environment
DIE-TA	Defence Information Environment - Technical Architecture (Australia)
DIF	Data Interchange Format
DIGEST	Digital Geographic Information Exchange Standard
DM	Data Management
DNS	Domain Name Service
DoD	Department of Defense
DSP	Directory Shadowing Protocol
DTA	Defence Technical Architecture
EDI	Electronic Document Interchange
EMC	Electromagnetic Compatibility
EPS	Encapsulated Postscript
FTAM	File Transfer And Management
GIS	Geographic Information System

HCI	Human Computer Interface
HO	Hydrographic Office
HTML	Hypertext Mark-up Language
HTTP	Hypertext Transfer Protocol
IER	Information Exchange Requirement
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPC	Inter-Process Communications
IPS	Internet Protocol Suite
IS	Information System
ISME	International Subject Matter Experts
ISO	International Standards Organisation
ISS	Infrastructure Strategy Study
IT	Information Technology
ITU	International Telecommunications Union
JANAP	Joint Army, Navy, Air force Publication
JTA	Joint Technical Architecture
JWID97	Join Warrior Interoperability Demonstration 1997
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LPD	Line Printer Daemon
MIME	Multipurpose Internet Mail Extension

MOD	Ministry of Defence
MS	Message Store; Microsoft
MTF	Message Text Format
NAT	Name Address Translation
NATO	North Atlantic Treaty Organisation
NFS	Network File Service
NITFS	National Imagery Transmission Format Standard
NNTP	News Network Transfer Protocol
NSAP	Network Service Access Point
NSIF	NATO Secondary Imagery Format
NT	(Windows) New Technology
NTP	Network Time Protocol
NWTDB	Naval Warfare Tactical Database
OA	Office Automation
ODA	Open Document Architecture
ODBC	Open Database Connectivity
OLE	Object Linking and Embedding
ONC	Open Network Computing
O/R	(X.400) Originator/Recipient (address)
OSI	Open System Interconnection
OSIPS	OSI Protocol Suite
OTHT-G	Over The Horizon Targeting - Gold

PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
POP3	Post Office Protocol (Version) 3
RAT	Reverse Address Translation protocol
RDA	Remote Data Access
RDBMS	Relational DBMS
RPC	Remote Procedure Call
RTF	Rich Text Format
SGML	Standard Generalised Markup Language
SMB	Server Message Block
SMTP	Simple Message Transfer Protocol
SSL	Secure Sockets Layer
TCP	Transport Control Protocol
TLB	Top Level Budget (Holder)
TLSP	Transport Layer Security Protocol
TRM	Technical Reference Model
TSG	Theatre Systems Group
TSIX(RE)	Trusted Systems Interoperability Group (Restricted Environment)
UA	User Agent
UDP	User Datagram Protocol
VLSM	Variable Length Sub-net Masking
W3C	World Wide Web Consortium

WAN	Wide Area Network
WINS	Windows Internet Name Services
WML	Wireless Markup Language
XHTML	eXtensible Hypertext Markup Language
XML	eXtensible Markup Language

A. Assessment: supporting information

A.1 Introduction

A.1.1 This annex provides additional explanatory material in support of the assessment in Chapter 6. Only significant or contentious assertions are given further justification here; points in this annex are cross-referenced to the assessment Table 6.

A.2 Office Automation

A.2.1 For *interoperability* purposes, there is no need to standardise on a particular OA package; a document file format can be selected as a standard for interchange purposes. (There might be other legitimate reasons for selecting a standard OA package, e.g. to minimise maintenance and support costs.) Of course the selected file format might not currently be supported *effectively* on more than one package, leading to a preference for that package; however, to exclude other packages completely and permanently presupposes that there will never be effective alternative. Moreover, selection of a single package will unduly constrain those systems that are not Windows-based (e.g. UNIX, where emulation is not a generally effective solution, or mainframe-based systems).

A.3 OSI application layer service elements

A.3.1 The OSI upper layer services and protocols are not widely used, except for certain specific OSI applications that call them up as part of a common profile (e.g. X.400 and X.500 services). Application developers in other areas seldom use OSI protocols, normally electing to use RPC or application-specific protocols (e.g. for transaction management). Therefore the only requirement for standardisation of OSI upper layer protocols and services within the CITA arises in the context of specific messaging and directory profiles. FTAM is the only other OSI application layer protocol that might in the future be sufficiently widely used to justify inclusion within the CITA.

A.4 Enterprise-level data management

A.4.1 For inter-nation interoperability purposes, it is only necessary to standardise the definitions of information exchanged between systems in different nations and, even then, it is sufficient to standardise external schema representations only.

A.4.2 There are other reasons why more extensive standardisation of data might be advantageous (e.g. application portability) but these concerns are outside the scope of the CITA.

A.4.3 To support unanticipated exchanges of information (for which provision was not made at design time), it would clearly be beneficial if the format and meaning of that data had been agreed in advance. However, such universal standardisation is highly costly and its benefits are at best difficult to quantify (and at worst might never materialise). Speculative standardisation also has the disadvantage (demonstrated repeatedly by previous 'open' computing initiatives) that the standards produced are seldom usable; by its very nature the process for production of such standards is pre-emptive and therefore unable to take into account specific requirements. Subsequent failure to adopt those standards leads to their being undermined and eventually displaced altogether by de facto substitutes.

A.4.4 Nevertheless, the increasingly unpredictable nature of military operations, together with changing concepts of operations demanding increased interchange of data from the strategic to tactical levels, suggests that local interchange agreements (e.g. within a nation, bilateral between systems) will become increasingly unsustainable. Emphasis will need to shift towards CCEB-wide agreements, encapsulated within the CITA.

A.4.5 These issues, and the wider role of data management within CCEB must be reviewed. The eventual scope and form of the CITA will therefore be influenced by this work.

A.4.6 It has been suggested in some quarters that object-based approaches providing data encapsulation ('data hiding') can obviate the need for the widespread data standardisation to support remote data access, and thus that any other approach to data management may be inappropriate once extensive use is made of object-based mechanisms. Both of these assertions are true to a degree, but need qualification. This Data encapsulation does not remove the need to standardise the data that *is* exchanged between systems. Moreover, encapsulation only limits the degree of inter-system data agreement needed if the specific requests for information exchange (the 'methods' in object terminology) can be determined in advance. Therefore, even if object mechanisms are widely employed it will still be necessary to standardise core data elements relevant to inter-domain interoperability within the CITA, and to pre-determine the nature of requests for information exchange.

A.5 Database to database replication

A.5.1 Database to database replication excludes simplistic transfer mechanisms using business-transaction-oriented data interchange formats, e.g. ADatP3; such interoperability mechanisms are considered under another heading. The mechanisms considered under this category are the more sophisticated protocols employed within

commercial products capable of transaction management, selective attribute-based replication, etc.

A.5.2 At present, each commercial database product provides its own proprietary replication mechanisms. Effective standards do not exist for protocols, nor for the data formats employed, or the integrity services provided. Replication between dissimilar products is only possible to a limited degree. It would be possible to adopt a proprietary product as a CITA standard but no product currently has sufficient market dominance to justify this (i.e. the disadvantages of product standardisation would outweigh the advantages of inclusion of the service within the CITA).

A.6 Remote data access

A.6.1 Each individual database or 4GL product uses its own standard for remote data access; there are also proprietary middleware products that effectively mediate between different database client and server products. There are effective APIs in the Windows and UNIX environments; ODBC provides an API in the Windows client and server environments as well as in the UNIX server environment; currently there does not appear to be an ODBC product available for the UNIX client environment. However, there are no acceptably open data access protocols. (RDA is not a credible standard.) Unfortunately, individual projects with data access requirements will either need to agree compatible client and server products, or agree the use of whichever middleware product best meets individual project requirements.

A.6.2 An alternative approach, now gaining wide acceptance on the Internet, is to represent simple database structures as hypermedia objects instead of relational databases. This then allows a standard protocol (i.e. http) to be used for database browsing and access. A similar approach allows an http front-end to be fitted onto a conventional relational database product, allowing universal access to web browser clients. Many database manufacturers now market utilities that provide this capability but these only offer access to a limited subset of normal DBMS functionality. These could represent a valuable part of a future CITA but at present the degree of standardisation and limited functionality mean that they are unable to satisfy the full range of data access requirements.

A.7 OA interchange formats

A.7.1 De jure document interchange standards have neither the richness nor the product support to be credible interchange standards. (An exception to this is HTML, a specific application of SGML, which is considered under a separate category.) Interchange between different OA applications (e.g. between Microsoft Word and Applixware) is generally much more effective where one of the proprietary formats is used rather than where vendor-neutral formats (e.g. RTF) are used.

A.7.2 More recently products (such as VMWare) have emerged that allow the Windows operating system to be run in a UNIX environment thus permitting native Windows applications to be hosted. Although this is not a new idea, it is only recently that the products have become sufficiently mature and an acceptable performance achieved. It is, therefore, a practical option for high levels of cross-platform interoperability to be achieved by using the same applications on both Windows and UNIX platforms.

A.8 Hypertext interchange formats

A.8.1 The assertion made in table 5 presupposes the existence of a CCEB Intranet, which is widely called for in many quarters but cannot exist before a number of significant requirements and security issues are resolved.

A.8.2 Independently, the requirement for document interchange can be satisfied to a degree by the adoption of hypertext formats as interchange formats. This offers more limited functionality than the OA formats themselves but can be useful in those circumstances where native support for the OA formats is not available.

A.9 Messaging

A.9.1 The X.400 functional model and a typical client/server messaging configuration are shown in the figure A-1.

A.9.2 Whilst many mail server products support X.400, this is generally only for server-to-server connections (i.e. the products support the X.400 P1 protocol but not the P3 or P7 protocols). Moreover, whilst X.400-compliant UA and MS components are commercially available, they offer very limited functionality compared with mainstream COTS messaging products (which often include Groupware functionality as well as messaging functionality); this would force many systems adopting X.400-compliant MS and UA products to provide more mainstream products *in addition*. A standards strategy which forces projects down this route is clearly not sensible.

A.9.3 For interoperability between domains, conformance with the P1 protocol standard (plus body part formats) is necessary but conformance with other protocol standards (i.e. P3, P7) is not[1].

---

1 It is assumed that domain boundaries are organised such that direct access by a mail client in one domain to a server in another domain is not required; this will usually be precluded on security grounds in any event.

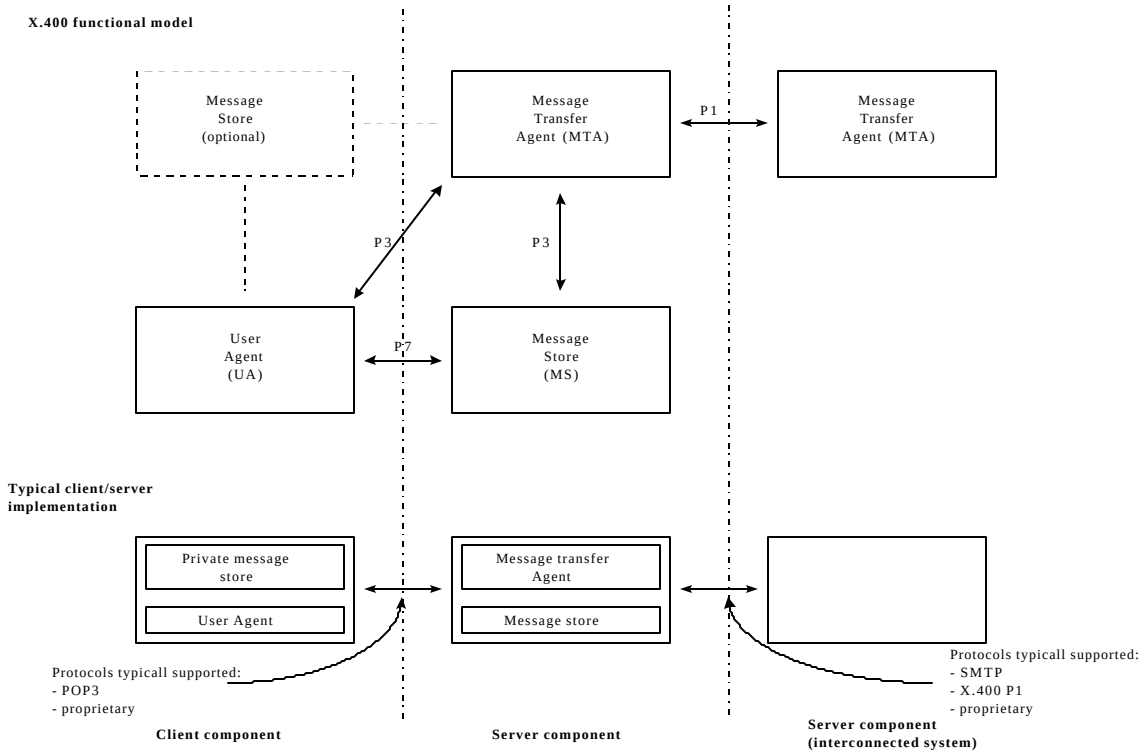

Figure A-1 X.400 functional model

A.10 Directory

A.10.1 Projects' selection of a directory product is usually dictated by their choice of messaging product (e.g. Microsoft Exchange provides the directory as well as messaging service). So, although X.500-compliant products are commercially available, they do not represent a viable solution for the majority of projects. The data interchange capabilities supported by X.500 (e.g. directory chaining and shadowing) are usually supported by commercial products, but only within proprietary 'islands' using proprietary protocols. Therefore these aspects cannot realistically be standardised and should therefore (for the present at least) be excluded from the CITA.

A.10.2 Nevertheless, it is desirable that directory interchange protocols are included in the CITA in the medium-term, hence the emergence of *well-supported* open standards (such as LDIF) needs to be monitored. It will be important for CCEB to ensure that its policy over directory services is not divorced from commercial trends thus potentially preventing projects from adopting mainstream COTS products. It is possible that third-party products will emerge that are capable of achieving interworking between proprietary directory chaining/shadowing protocols and X.500 protocols. Availability of suitable products would allow these services to be brought within CITA scope.

A.11 Key management and distribution

A.11.1 No Defence IT systems presently employ asymmetric cryptographic algorithms and their future use is dependent upon the approval of algorithms for Defence use and the existence of suitable implementations. Therefore there is no present possibility of standardisation of an asymmetric key distribution service within the CITA (although open standards for such services, and widely used implementations of commercial algorithms, do exist). There are no acceptably open standards for the distribution of symmetric encryption keys (other than in conjunction with a wider asymmetric distribution service); therefore these also cannot be standardised within the CITA.

A.11.2 Clearly, however, if widespread use is to be made of cryptographically-delivered security services within other CITA services (notably messaging), there will ultimately be a requirement to standardise key distribution services. Progress on this front within the CITA is contingent upon current secure messaging initiatives (e.g. CASM) coming to fruition.

A.12 System management

A.12.1 This category is taken to mean the exchange of management information and services between systems in order to permit remote management or the management of several systems as a single whole[2].

A.12.2 No requirements have been identified for exchange of system management services between domains, and no future requirement seems likely to emerge. In any event, the lack of open standards would preclude these services being adopted in the CITA even if requirements were to become apparent. With an ever-increasing level of integration between CCEB CIS, system management responsibility is one of the few remaining criteria by which system boundaries are drawn. Strong control and management of a system is a prerequisite to the implementation of an effective security policy, which will also limit the degree to which management control can be federated among CCEB CIS.

A.13 Network management

A.13.1 This category is taken to mean the exchange of management information and services among end-systems and between end-systems and the wide-area communications

---

2 The management of interconnected systems in a coordinated manner to maintain interoperability (e.g. by carrying out software upgrades simultaneously to minimise backwards compatibility problems) will be necessary but is expected to be achieved by procedural means and is therefore outside CITA scope.

infrastructure in order to permit remote network management or the simultaneous management of several systems' local network components.

A.13.2 Again, strong local network management control is usually required to enforce local system security policies. Therefore, even though open standards exist in this area, no requirement for CITA standardisation has been identified. The only identified requirements in this area fall under other CITA categories (i.e. name and address allocation, internetworking protocols).

A.14 Local area networking

A.14.1 LAN standards are outside CITA scope because, by definition, a LAN must be internal to individual CCEB nations. Requirements occasionally arise for co-located systems to share the same physical LAN or to interconnect via attachment to a common LAN and hence be within the CITA scope:

- sharing LANs between independent systems reduces the costs of network installation and operation;

- where systems interwork, attachment to a common LAN could be the most effective solution though alternative methods of interconnection (e.g. via the wide-area network or via a local router) also exist. It is the choice of Internet protocol, rather than LAN medium, which makes interconnection possible.

A.15 Name services

A.15.1 Irrespective of whether X.500 services are provided directly, an X.500 naming policy will be required because X.500 names are used in X.509 certificates; these in turn are likely to be used in the CITA secure messaging profile.

A.16 Object Interchange

A.16.1 There are a number of competing standards for the interchange of objects between applications. All are emerging and there is no clear leader at present. There are no open standards. Most use remote procedure call (RPC) mechanisms to effect distribution of computational effort, the exception being Java The main contenders are:

A.16.2 Active X: this is Microsoft's standard based on its Distributed Component Object Model (DCOM) technology. It is being ported to most UNIX platforms.

A.16.3 CORBA: Common Object Request Broker Architecture is the Object Management Groups (OMG) attempt to introduce open standards into distributed computing. The OMG is a consortium of companies developing these standards but relying on individual companies to provide products.

A.16.4 DCE: Distributed Computing Environment is the Open Group's standard for distributed computing.

A.16.5 JAVA: Sun's attempt to produce truly portable programs has been taken up by a number of vendors. It uses a Java Virtual Machine (JVM) to execute Java code. Any platform that support a JVM should (in theory) be able to execute any Java program. Java programs can be distributed (and executed) across a federation of computing platforms. It should be noted that practice and theory have not yet fully converged.

A.17 Alerts services

A.17.1 An alert is a message which can contain multiple information types, as with other messages. Alerts services are normally distinguished from messaging services on the basis that they:

- are commonly sent on an all-informed or multicast basis and, on efficiency grounds, use different distribution mechanisms;
- need to be brought directly to the attention of the user, and usually require positive acknowledgment before other tasks can be continued.

A.17.2 Requirements for alerts arise in two ways in CCEB CIS:

- for distribution of urgent system management messages or instructions;
- for rapid dissemination of operationally significant information such as warnings.

A.18 Architectural Concepts

A.18.1 The CITA is predominately based upon the concept of a federation of fixed and mobile systems which together form a CCEB Intranet. Embodied within the CITA, therefore, is the concept of a technical architecture that has the Internet standards and protocols at its heart. Central to these is the four-layer TCP/IP protocol stack which many applications (e.g. SMTP email) are designed to use. The layers are:

- communications network layer;

- Internet Protocol (IP) layer;
- TCP and UDP layer;
- applications layer.

A.18.2 Other mandated applications, however, (e.g. X.400 messaging) have been designed to use the seven-layer OSI protocol stack (see section A.3) which has the following seven layers:

- physical layer;
- data link layer;
- network layer;
- transport layer;
- session layer;
- presentation layer;
- application layer.

A.18.3 These two models align as shown in figure A-2 .

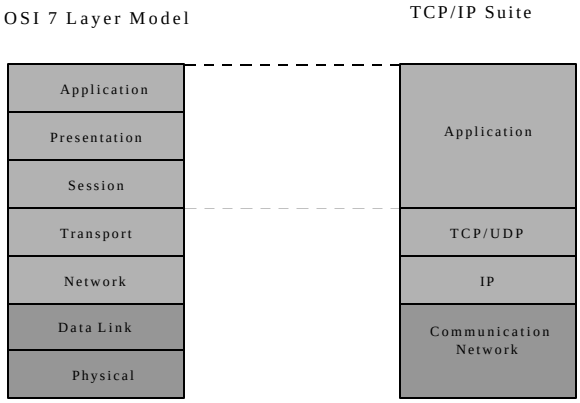

Figure A-2 OSI and TCP/IP Protocol Stacks

A.18.4 This creates a dichotomy in the CITA that requires ISO transport services to be layered on top of TCP/IP (as defined in RFC 1006). These are embodied in the CITA,

although their purpose may not be immediately obvious, so that ISO-based applications such as X.400 and FTAM can be supported.

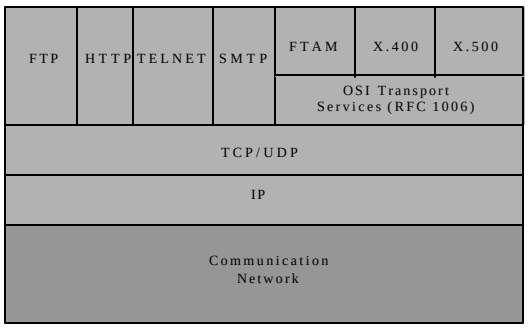

Figure A-3 OSI and TCP/IP Applications

A.19 Coalition Wide Area Network (CWAN) Management

A.19.1 The CWAN, along with associated systems, applications, and services; is managed with remote monitoring and control capabilities via the Coalition Communications Control Center (CCCC or QuadC) and the Alt CCCC. It has links that electronically exchange information between management systems at all levels.

A.19.2 CCCC Management Overview

A.19.3 The purpose of the CCCC is to provide seamless, secure information products and services to JWID participants, especially warfighters, in support of decision-making and mission accomplishment.

A.19.4 Within the Commander-in-Chief(CINC), Service and Agency (C/S/A) organisations today, network, system, application, and service management functions are performed by a wide range of individuals, activities, and organisations. These management and/or controlling functions are performed at all levels. However, in the JWID environment, these functions must be performed at the CCCC and Alternative CCCC (ACCCC). These control centers can be located within any domains. While it can provide virtual presence at any location on the network, each control center can perform independent and integrated management functions supporting communications and information systems. These systems include local area network (LAN) management and the

CWAN. Each provides operational support essential to sustaining the CWAN. The CCCC CONOPS is aimed at realigning, consolidating, and integrating these functions to fulfill the following goals:

A.19.5 The CCCC structure enables the capability to:

- revolutionize information exchange across the CWAN;
- strengthen the ability to apply computing, communications and information management capabilities effectively to accomplish the JWID mission;
- significantly reduce information technology burdens on operational and functional staffs; and
- facilitate the capability for the operational and functional staffs to access, share and exchange information worldwide, with minimal knowledge of communication and computing technologies.

A.19.6 A wide range of individuals, activities and organizations perform network, system, application and service management functions within C/S/As, at all levels. However, in the JWID environment, these functions must be performed at the CCCC and Alternative CCCC (ACCCC). These control centers can be located within any domain. While it can provide virtual presence at any network location, each control center can perform independent and integrated management functions supporting communications and information systems. These systems, including local area network (LAN) management and the CWAN, provide operational support essential to sustaining the CWAN. The CCCC CONOPS realigns, consolidates and integrates these functions to fulfill the following goals:

- Enhanced C4IFTW support
- Secure operations
- Coordinated problem resolution
- Shared management information (status, availability)
- Global visibility
- Interoperable resources.

A.19.7 **CCCC Management Functions**

A.19.8 **Fault management** is the detection, isolation, and correction of problems in, or abnormal operation of, disabled network or information processing system components. Appendix A explains the functions associated with fault management.

A.19.9 **Configuration management** identifies, exercises control over, collects data from, and provides data to networks for the purpose of preparing for, initialising, starting, providing for the continuous operation of, and terminating interconnection of processing services. Configuration management functions and tasks may overlap with both fault management and performance management, along with long-term planning of the network's topology, the information processing system's configuration, and inventory. Appendix A of the CCCC CONOPS summarises the functions associated with configuration management.

A.19.10 **Performance management** monitors and controls the quality of network communications or information processing. It involves the processes of monitoring and analysing; tuning and controlling; and reporting on network or information processing system components and on the network or information processing system as a whole. Appendix A of the CCCC CONOPS summarises the functions associated with performance management.

A.19.11 **Security management** includes the confidentiality, authenticity, and integrity of network management data such as routing tables, access lists, audit data protection, and accounting and billing information. Security management is the management of the following network or information processing system security services: authentication, access control, encryption, and audit trail. Security management controls and monitors the mechanisms that protect selected network or information processing system resources and user information, or security objects. Security management includes controlling access to resources, archiving and retrieving security information, and managing the encryption process. The management functions associated with security management are found in Appendix A of the CCCC CONOPS.

A.19.12 The CCCC has oversight responsibility for the entire CWAN and interfaces directly with the network participants. The CCCC will provide the overall management control and technical direction of the CWAN. As the direct interface for the customers, the CCCC performs demonstration participant assistance and provides contemporary operational network services. It serves as a central point of contact in operational and emergency provisioning aspects of customer service when the needs are beyond the capability of the site engineers. Operational policies and procedures for the CCCC are under development. Additional C/S/A policies will also apply based on the mission

being supported by the CCCC. The CCCC is responsible for the following functional responsibilities and requirements:

- Providing CWAN policy, standards, and guidance for systems and network management

- Monitoring status, in real-time or near-real-time, of CWAN applications, networks systems, and JJPO concerns

- Providing access to Global CWAN status for authorized users as required

- Implementing tool suites, processes, and databases that provide the "global" view for applications, systems, and network assets

A.19.13 The vulnerabilities of networks to information security attacks dictate that network management and information security management information be shared across multiple communities of interest. The end-user/JWID customer, upon discovering an information security anomaly, would report it to the CCCC, which would report enterprise-level anomalies to the CTFC. Anomalies to circuits or systems that are not of CTFC interest would be processed and resolved at the CCCC. The CCCC and/or ACCCC would be responsible for aggregating information reported to them and passing it to the CTFC and JJPO for fusion. Doctrine associated with such actions are under way to address, refine, and integrate the reporting structures.

A.19.14 Successful CCCC operations rely on compatibility, interoperability and integration of policies, procedures, standards and tools.

A.20 Deployed CIS

A.20.1 The CITA has focused on CIS that are principally static in nature and has given limited consideration to the operation of deployed CIS. The constraints that exist in theatre typically relate to the communications systems (i.e. bandwidth, availability, quality of service) and must be resolved appropriately. The CITA has a part to play in resolving these issues.

A.20.2 It is now considered possible that coalition forces may federate their CIS in a deployment so that local autonomous services are provided within the constrained environment. In other words, the coalition forces may interconnect systems or LANs locally 'on the ground' forming one or more sub-networks. This would also mean that one nation could be responsible for providing services such as Naming, Addressing and Directory to other nation's systems. In this case each nation's systems would have to conform to additional standards such as CIDR VLSM for sub-netting, DHCP for IP

address allocation and LDAP for directory access. This means that local services could be used thus reducing any dependency on premium resources such as long haul communications.

B. CITA Recommended Standards Profiles

B.1 Introduction

B.1.1 This annex provides the detailed profile of standards for the both the current and emerging CITA.

This page intentionally blank

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
1: Operating system services	Standards for the services provided by computer operating systems and the means of accessing them.	Not relevant to interoperability.	N/A.	N/A	Relevant to porting/reuse of applications software which can contribute to interoperability in some circumstances; however, there is no general inter-nation requirement for porting/reuse. It is anticipated, however, that Win32 or UNIX95 standards would be specified if a CCEB requirement were to arise.
2: User Interface Services	A miscellany of standards relevant to the Human-Computer Interface.	A few standards under this category are relevant to interoperability (eg remote presentation services); these are covered under other headings below (eg distributed computing). The remainder are not relevant to interoperability.	N/A.	N/A.	Relevant to people portability only.
HCI Toolkit	See above				
HCI Style Guide	See above				
Windowing	See above				
3: Network services					

Messaging (including military message handling)	Standards for services providing users with the means to create and transfer information in the form of messages to one or more recipients at local or remote locations. Messages are transferred in one or more store-and-forward hops. Text- and bit-oriented messages are covered separately in section 7.	Scope is limited to message transfer protocols and message content formats. Where attachments are to be exchanged, relevant data interchange standards also apply. Security services for messaging are considered separately.	**Organisational Messaging:** Message transport submission & delivery (P1/P3/P7) ACP 123 Annex C.(with STANAG 4406 Alpha Profile Set profile AMH91 (MA), plus support for the file transfer body part). Gateway between MMHS and ACP127 to be defined. Content Type (P772, ACP 123 Annex A, Annex B, Annex D) Message Store Attributes (P772, MS Attributes, ACP 123 Annex E, Annex F) **Interpersonal Messaging:** SMTP (RFC 821) + MIME (RFC 2045) (See notes.) **Naming and addressing:** ACP 133 for Directory Services; ACP 123 for Messaging Services;	N/A	X.400 is the most viable technical option for Organisational (high assurance) messaging. This is specified by the AIS ISME. AMH91 likely to include a file transfer body part. The requirement for interpersonal (email) messaging has recently been agreed. Internet-derived specifications SMTP and MIME are recommended. A naming and addressing policy and schema for email will be required, as is a security protocol; these could be extensions to ACP 133 and ACP 120 respectively.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
3: Network services (cont)					
Directory	Services for the provision of information relating to all forms of communications and information services including the support messaging and security services.	CITA scope covers a scaleable directory system in support of many forms of communication including, but not limited to, organisational communication (e.g. Postal), Telecommunications, Messaging, Secure Messaging, User Authentication and information relating to Task Force organisation and tactical (mobile) units (e.g. ships). The directory must support the public key infrastructure required by allied security policy.	ACP133 (based on X.500 1992 with some 1997 extensions). LDAP v3 for deployed networks (see para A.20)	CITA will monitor developments in national directory service projects. An SMTP addressing schema will need to be formulated as per ACP133.	Note that directory services require the implementation of a CITA naming policy covering X.500 names (see naming and addressing management below).

Naming and Addressing services	Services for resolution of computer or server names into specific network-level addresses.	Within CITA scope.	DNS (RFC 1034, 1035) Bind v 8.2 or later Internet domain naming policy. NAT (RFC 1631) See notes.	RAT (IETF draft) for deployed mobility. See notes	DNS required for IP internetworking. Note that a CITA naming policy is required for domain names in order to prevent domain name conflicts. The increasingly widespread use of Windows NT-based networks within CIS makes a policy for consistent NT-domain naming highly desirable. Such a policy does not presently exist. In the medium term Windows 2000 is likely to replace NT. Its domain structure follows the DNS hierarchy thus reducing the need for a separate domain policy. Name Address Translation (NAT) is necessary for cases where the IP addresses internal to a system cannot be used outside that system because of the risk of conflicts (e.g. systems using private Internet addresses such as 10.x.y.z). Reverse Address Translation protocol (RAT) is a mechanism for deploying mobility support by riding on NAT.
Remote terminal services	Remote terminal is specifically limited to character-mode terminal emulation. (Graphical-mode is covered under other categories.)	Within CITA scope.	TELNET (RFC 854/855)	TELNET is expected to remain a current standard as long as there is a requirement to support connections to legacy systems.	Specific interoperability requirements with legacy systems will entail provision of remote terminal services but the legacy system will determine the particular protocol used in each case (e.g. TELNET, VT220, VT320, ... , OPSXE, etc).

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
3: Network services (cont)					
File transfer protocols	Services for transferring the contents of files between systems.	Within CITA scope.	FTP (RFC 959) and HTTP v1.1 (RFC 2616) for file transfer - (Netscape Navigator and MS Internet Explorer and their interoperable proprietary extensions). FTP products that implement the 'Restart' elements of RFC 959 for file transfer in constrained environments. For HTTP this is in practice Netscape Navigator v4 and MS Internet Explorer v4, and their interoperable proprietary extensions.	FTP and HTTP are expected to remain current standards for the foreseeable future. The applicability of Trivial FTP and Enhanced Trivial FTP needs to be monitored. The HTTP Distribution and Replication Protocol also needs to be monitored.	FTP is a complex, robust protocol designed to transfer any type of file between computers. It can be used either as a stand-alone application or as middleware. HTTP is a protocol specifically designed for simple and efficient transfer of small files, typically HTML documents and multimedia files. It is in practice Netscape and MSExplorer, and the interoperable proprietary extensions common to both. FTP and HTTP are mandated standards for file transfer services. However, FTP and standard HTTP, if authenticated, require passwords to be transmitted in clear over a network which may preclude their use in many circumstances. There are proprietary extensions to HTTP (but not FTP) which can overcome this, satisfying local security policy restrictions and allowing a standard interface to be exposed at system boundaries (eg through a firewall) but none is acceptably open. For constrained environments (where communication links may be unreliable) FTP with restart is recommended as the file transfer standard. It has the ability to restart an interrupted transfer from the interruption point.
ISO services on top of the transport layer	Services and protocols at application, presentation and session layers.	Within CITA scope.	RFC 1006. (See note.)	N/A.	OSI upper layer protocols only, as cited within other CITA services (eg messaging & directory). IPS equivalents are explicitly identified elsewhere in this table. RFC 1006 specifies use of OSI applications over TCP/IP (See Section A.18).

Socket services.	APIs providing access to internet protocols (i.e sockets such as WinSock) and associated applications. Web browsers are covered under hypertext transfer protocols and hypertext document formats.	Not relevant to interoperability.	N/A.	N/A.	These service providers sit at or above the application later of the TCP/IP protocol stack. Their relevance is primarily for application portability.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
4: Communications					
Networking					

Telephony	Services for voice encoding across both analogue and digital dial-up connections. Includes modem services.	Within CITA scope	**Secure telephony:** STU-IIB compliant equipment. **Insecure telephony:** Standards selected from ITU-T Recommendations: Series E - Overall network operation, telephone service, service operation and human factors; Series G - Transmission systems and media, digital systems and networks; Series P - Telephone transmission quality, telephone installations, local line networks; Series Q - Switching and signalling; Series V - Data communication over the telephone network. V.34 for modems. V.42 for communications compression	The STU-IIB standard is soon to be replaced by STE (Secure Telephone Equipment). Voice-over-IP standards are experiencing growing market take-up and should be monitored. As the V.90 modem standard (56 Kbits/sec) becomes widely adopted, the CITA specification will be upgraded to this standard.	Incompatibilities between A-law and µ-law voice encoding standards are normally resolved by the A-law-based telephone exchange.

Wide area networking	Standards for the transfer of data across wide area networks including X.25, Frame Relay, ISDN, B-ISDN (ATM) and SONET	CITA scope limited to specification of the services offered by the wide-area communications infrastructure.	**X.25:** X.25 support required for legacy networks into next century. **X.121 addressing policy:** X.121 registrations required to support X.25. **ISDN:** ITU-T Series I Recommendations. **B-ISDN (ATM):** ITU-T Series I Recommendations ATM Forum af-standards for physical and adaption layers. LAN Emulation (LANE) af-0087.000 v2.0. **SONET/SDH[3]:** ANSI T1.105.	It is the CITA view that ATM will eventually emerge as the preferred single standard.	CITA standards must reflect the networking technologies and services provided within the CCEB communications infrastructure. CITA scope limited to specification of the services provided by the wide-area communications infrastructure (ie internetworking protocols, data link and physical layer specifications at point of attachment). No use of OSI network-layer protocol assumed. X.25 support required for legacy networks into next century (hence continuing need for X.121 registrations).

3 SDH is the ITU-T standard for packaging cells over fibre-optic bearers at data rates of greater than or equal to 155.52 Mbit/s. SDH is a physical layer technology capable of being used with systems supporting a variety of protocol stacks and providing a path for unlimited upgrades at intervals of 51.8 Mbit/s up to a maximum of 10 Gbit/s. SONET is the North American standard equivalent to SDH which provides data rates starting at 51.8 Mbit/s and increasing by multiples of 51.8 Mbit/s. Whilst SONET and SDH have many similarities, there are some important differences relating to data rates and multiplexing strategies which may prevent interoperability. SDH Networks can only interoperate successfully with SONET networks if appropriate data rates and multiplexing strategies are selected.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
4: Communications (cont)					
Point-to-point	Services providing full duplex, synchronous or asynchronous, point-to-point communications.	Within CITA scope.	RFC 1661/1662 (PPP) RFC 1332 (PPP Internet Protocol Control Protocol (IPCP)) RFC 1989 (PPP Link Quality Monitoring) RFC 1994 (PPP Challenge Handshake Authentication Protocol (CHAP)) RFC 1570 (Link Control Protocol (LCP) Extensions).	None at present.	
Tactical data links	Links supporting the transfer of tactical information between coalition forces.	Within CITA scope.	**Link 11** STANAG 5511 annex B, Radio performance & protocols; vol.2, Link 11B Waveform protocol changes. MIL-STD-118-2031a, Conventional Link 11 Waveform 16 tones. SPAWAR-5-850, Single tone Link 11 Waveform. **Link 16** STANAG 4175 edition 1. **Link 22** UHF: STANAG 4372 (Saturn); Saturn can also carry Link 11 and Link 16 messages. HF: STANAG 4444 (Slow hop ECCM). **Link forwarding:** STANAG 5616.	VMF.	

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
4: Communications (cont)					
Network Interconnection					
Internetworking	Standards for the transfer of data across LAN/WAN and LAN/LAN boundaries.	Within CITA scope.	IPv4 (RFC 791) moving to IPv6 (RFC 1883) and the following associated standards: IP Sub-netting (RFC 950) Broadcasting Internet Datagrams (RFC 919) Broadcasting Internet Datagrams in the presence of subnets (RFC 922) Internet Control Message Protocol (ICMP) (RFC 792) Awaiting CCEB policy on IP addressing. DHCP (RFC 2131) for deployed networks. See para A.20.	IPv6 (RFC 1883).	The CITA standards must reflect the networking technologies and services provided within the CCEB communications infrastructure. CITA scope limited to specification of the permissible modes of LAN/WAN and LAN/LAN interworking for the purposes of interconnection.
Transport	Services providing user access to internetworking services and end-to-end quality enhancement.	Within CITA scope.	TCP (RFC 793) UDP (RFC 768).	N/A	No use of OSI transport-layer protocol assumed.
Router services	Standards for routers used to interconnect various subnetworks and end-systems.	Within CITA scope.	RFC 1812 - Requirements for IP Version 4 Routers Border Gateway Protocol 4 (BGP-4) for exterior gateway routing. (RFC 1771) OSPF v2 (RFC 2328) See note.	RFC 1933 (Transition Mechanisms for IPv6 Hosts and Routers)	OSPF v2 is specified because of its auto-discovery function.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
4: Communications (cont)					
Bearers					

SATCOM	Standards for the transfer of data across SATCOM links including UHF, SHF and EHF.	Within CITA scope.	**General** MIL-STD-188-146 Interoperability And Performance Standards For Satellite Communications, 15 June 1998. **UHF** MIL-STD-188-181A, Interoperability Standard for Single Access 5-kHz and 25-kHz UHF Satellite Communications Channels, 31 March 1997. MIL-STD-188-182A, Interoperability Standard for 5-kHz UHF DAMA Terminal Waveform, 31 March 1997. MIL-STD-188-183, Interoperability Standard for 25-kHz UHF/TDMA/DAMA Terminal Waveform, 18 September 1992; with Notice of Change 1, 2 December 1996 (STANAG 4231). MIL-STD-188-184, Interoperability and Performance Standard for the Data Control Waveform, 20 August 1993. MIL-STD-188-185, DoD Interface Standard, Interoperability of UHF MILSATCOM DAMA Control System, 29 May 1996. **SHF** MIL-STD-188-164, Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, 13 January 1995. MIL-STD-188-165, Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), 13 January 1995. **EHF** MIL-STD-1582D, EHF LDR (Low Data Rate) Uplinks and Downlinks, 30 September 1996; with Notice of Change 1, 14 February 1997 (STANAG 4233). MIL-STD-188-136, EHF MDR (Medium Data Rate) Uplinks and Downlinks, 26 August 1995; with Notice of Change 1, 15 August 1996, and Notice of Change 2, 14 February 1997 (STANAG 4522).	N/A	STANAG 4522 is an initial draft which has been derived from MIL-STD-188-136. For any access to the SATCOM frequency spectrum, co-ordination of frequency assignments is required in support of operations. For Coalition forces, this is achieved through the ACP190 'Guide to Frequency Planning'. This document identifies the processes to follow in order to make the required SATCOM links.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
4: Communications (cont)					

Radio	Standards for the transfer of data across Radio links including VLF, LF, HF, VHF, UHF and SHF.	Within CITA scope (see note).	**LF/VLF** MIL STD 188-140A, Equipment Technical Design Standards for Common Long Haul/Tactical Radio Communications in the LF Band and Lower Frequency Bands, 1 May 1990. **HF** MIL STD 188-141A , Interoperability and Performance Standards for Medium and High Frequency Radio Equipment Standard. STANAG 4203 Technical standard for single channel HF radio equipment. **VHF** MIL STD 188-242, Tactical Single Channel (VHF) Radio Equipment. STANAG 4204 Technical standard for single channel VHF radio equipment. **UHF** MIL STD 188-243, Tactical Single Channel (UHF) Radio Communications. STANAG 4205 Technical standard for single channel UHF radio equipment. **SHF** MIL STD 188-145, Digital Line-of-Sight (LOS) Microwave Radio Equipment. **CNR (Voice only)** CNRs are only interoperable for fixed frequency (VHF) voice communications only. There are no commonly agreed standards for frequency agility. The standards are: QSTAG 734 (STANAG 4204) Technical Standards for Single Channel VHF Radio Equipment. QSTAG 1108 (STANAG 4197A) Common Critical Crypto Standards for Single Channel Communications (Voice, Teletype and Data) for VHF CNR.	N/A	As for copper/fibre-based bearers except encompassing non-physical bearers such as VLF, LF, HF, VHF, SHF etc. For any access to the radio frequency spectrum, co-ordination of frequency assignments is required in support of operations. For Coalition forces, this is achieved through the ACP190 'Guide to Frequency Planning'. This document identifies the processes to follow in order to make the required radio link bearers available.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
4: Communications (cont)					
Radio (cont.)			**Data modems** MIL-STD-188-110A Interoperability and Performance Standards for Data Modems. STANAG 4285 Characteristics of single tone modems for HF radio.		
Cable	Standards for the transfer of data across copper and fibre links including Optical, Shielded Twisted Pair (STP) and Unshielded Twisted Pair (UTP)	Within CITA scope (see note).	RS232, RS422, RS423; EIA-4920000-A, EIA-5090000; Other standards covered under wide area networks.	N/A.	For Systems to achieve any level of interoperability there must some form of physical interconnection. Such interconnection may involve the use of copper or fibre-based bearers. There is a wide range of standards in use within the CCEB nations. The role of the CITA is to encompass standards that could exist between rather than to define new ones. RS232 is included mainly for its commonality amongst legacy systems. It is generally superceeded by RS422/423.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
5: Distributed computing					
Distributed database management services	Services for maintenance or querying of databases distributed over multiple physical locations.	Covered under nation level data management	See section 6.		
Distributed Process	Services supporting remote procedure calls.	Outside scope of current CITA. Potential relevance to emerging CITA, subject to evidence of an inter-nation requirement and resolution of security issues.	None.	None at present. Emergence of requirements for use of RPC needs monitoring.	CORBA, IORPC, ONC+ RPC, DCE RPC and Active-X are all interoperable to an extent but not in a secure manner. Therefore future inclusion dependent also upon inclusion of relevant security services.
Remote presentation services	Protocols permitting graphical user interfaces to execute remotely from the client application (e.g. X11).	Outside CITA scope.	None.	None.	The ability of a user to render a remote application's GUI display on a local workstation may become a future a requirement. Technology has existed for some time that enables users to render UNIX displays on NT workstations. Technology to allow the rendering of NT displays on UNIX workstations has existed but not been part of main stream developments. More recently, however, the appearance of Windows NT Terminal Server Edition (Hydra) has brought such technology into a main stream product. Further, these services are planned to be available in Windows 2000 (NT v5.0).
Distributed file services	File sharing protocols.	Outside CITA scope.	None.	None.	

Distributed time services	Protocols for synchronisation of system clocks.	Outside CITA scope (see notes).	None.	If a requirement is forthcoming then NTP V2 (Network Time Protocol Version 2) RFC 1119 would be the recommended standard. NTP V3 (RFC 1305) is currently a draft standard. Also, to support the security services, the use of UTC and Generalised Time should be included.	The Common Security Protocol (CSP) detailed in ACP 120 identifies a number of security services that require a time stamping service. Also the need to synchronise X.500 directories across nations (because of Certificate Revocation Lists) may require a time synchronisation protocol. The CMI WG and AIS ISME will provide necessary advice. Time issues regarding Y2K are relevant to interoperability in so far as it is necessary for end-systems to correctly interpret time information. Individual nations will normally be required to ensure that systems within their control are Y2K compliant. This may involve considerable cost and risk, particularly where legacy systems are involved.
Distributed print services	Protocols for transfer of print jobs from client to spooler/printer.	Outside CITA scope.	None.	None.	

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
5: Distributed computing (cont.)					
Distributed transaction processing services	Services for the management of transactions involving participants on different end-systems (eg remote database update and synchronisation).	Outside scope of the current CITA.	None.	None.	
Object Interchange standards	Formats relevant to the encoding of object structures used in distributed computing.	Within CITA scope. Other distributed computing mechanisms considered under distributed computing category in section 5.	CORBA/IIOP v 2.4; DCOM.	The range of standards needed may broaden in the medium term with the increasing trend towards executable content in Internet technologies. However, it is not possible at present to predict which standards are likely to dominate. Monitoring is required.	ActiveX is a potential candidate for the medium-term, subject to its satisfactory support in non-MS environments. See section A.16.
Distributed object services (Object middleware)	Services for location of, or access to, objects when distributed over a network.	Outside scope of the current CITA. Potential relevance to medium term, subject to evidence of an inter-domain requirement and resolution of security issues.	None.	None at present. The emergence of a requirement needs to be monitored.	Acceptably open standards are emerging namely Microsoft's COM/DCOM and the OMG's CORBA 2.0. It is unlikely that security considerations will permit distributed object services to be employed widely in the foreseeable future. Also, Middleware may not feature in all individual nation's technical architectures.
Distributed system management services	Services for the coordinated management of various distributed components within a system.	Outside CITA scope.	None.	None.	If a coalition or combined Intranet has to be managed on a long-term basis, it would be desirable if the management functions could be performed using suitable standards and tools, assuming security requirements could be met. The management of the CWAN is described in section 8.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
6: Data management services					
Remote data access	Services that allow client terminal to access data on a remote database server in a client/server environment.	Within CITA scope.	ODBC v 3 (ISO 9075-3). (see note)	JDBC.	There are no truly open standards for remote data access, however Microsoft's ODBC has cross-platform support. It is questionable whether in practice a client terminal on one nation's CIS system accessing data on another nation's server would be used (or permitted). It is more likely that a server-to-server transaction would be used JDBC (Java DBC); is currently emerging ;it should be monitored. HTTP-based access protocols are currently used across the Internet; they offer limited database functionality but should also be monitored.
CCEB-level data management	What would normally be described as data management but concerning only that data which it is necessary to share between CCEB nations. (Sometimes refered to as Enterprise-level data manangement)	Within CITA scope. Need for flexibility to meet unforeseen interchange requirements emphasises need for CCEB-wide agreements in preference to more local agreements wherever possible. Nevertheless, complete definition of all CCEB data will be very costly, and for the most part speculative. Therefore, CITA data definition should, at least initially, be limited where possible to those items where there is firm evidence of a current or likely future CCEB-wide requirement for exchange of that data.	Standards are yet to be defined. Current definition should where possible focus on those data items for which there is clear evidence of an inter-nation exchange requirement. These definitions should be maintained in a central repository to aid ready access and deconfliction.	Follow emerging CCEB policy on data management (see note).	Current CCEB policy is for data schema, syntax and semantics to be defined on a pan CCEB-basis. Newly emerging CCEB policy indicates that data management policy should concentrate on defining the top 100 data items. Any CITA recommendation must reflect consequent changes in policy of individual CCEB nations. There is a need to examine approaches to CCEB data management: the CITA recommendation must reflect any consequent changes in policy of individual CCEB nations. A specific policy for database key management will be needed as part of overall policy for CCEB-level data management.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
6: Data management services (cont.)					
Nation-level data management					
Data dictionary services	Software development support tools that facilitate the management and use of project data dictionaries.	Not relevant to interoperability, outside CITA scope.	N/A.	N/A.	These services are within individual nation CIS boundaries and are hence nation-specific.
Database management system services	Facilities provided by a conventional DBMS.	Not relevant to interoperability, outside CITA scope.	N/A.	N/A.	As above.
Database replication	Mechanisms for replication of data between DBMSs.	There is a potential CCEB-wide requirement for database-to-database replication in the medium term. However, the likelihood of an acceptably open standard that meets CCEB requirements becoming available in the medium term is small. Outside scope of the current CITA.	None.	None at present Monitoring is, however, required of the scale of the CCEB-wide requirement to determine if adoption of a bespoke solution is justifiable (and whether such a solution is likely to emerge from current initiatives). Any decision is will also depend upon progress made in this area by NATO.	Whilst there are some aspirations in the CCEB community to employ database replication as an interoperability mechanism between systems in different nations, the strength of the CCEB-wide requirement is not certain, nor are timescales clear. There are no acceptably open standards for data replication - each DBMS vendor offers a proprietary solution. Selection of a non-open COTS solution is a possible strategy (at least for benign communications environments), but the consequent requirement for the whole of the CCEB to adopt a single DBMS is not likely to be acceptable. None of the available proprietary solutions is feasible in a tactical environment. Work is currently underway in the ATCISS programme examining a custom solution; this might offer a solution in the medium- to long-term.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
7: Data interchange					
Document interchange standards					

Office Automation interchange formats	Formats used for interchange of documents between OA tools.	Within CITA scope.	**Primary Standard** MS Office 97 interchange formats (Word 97, Excel 97, PowerPoint 97, Access 97) **Secondary Standard(s)** Rich Text Format (RTF); Portable Document Format (PDF); Ascii (TXT) for constrained environments	MS Office 2000 interchange formats to replace MS Office 97 interchange formats as the primary standard.	The MS Office OA suite is likely to remain the dominant product in the medium-term, hence its inclusion in the CITA as the primary interchange format. Any successful competing OA package would need to provide ready migration and thus would need to support MS Office formats for several years. Several legacy OA packages are in current use but functionally limited converters are available for most formats. Rich Text Format (RTF) is a neutral document formatting language that is sometimes used to transfer word processing documents between heterogeneous WP systems, preserving much of the original format. Although RTF is proprietary to Microsoft, it is widely available and supported by products. Variations exist in the implementation of the standard by vendors thus limiting the usefulness of the standard. RTF documents are typically much smaller than their Word equivalents, making it more suitable for use over low bandwidth connections; zip compression will further reduce the overall size of most documents. Portable Document Format (PDF) is an Adobe proprietary standard. The free availability of readers (Acrobat) and the level of cross platform support make this a suitable candidate for inclusion in the CITA as secondary standard. MS Office 2000 is already emerging as a replacement for MS Office 97, and is likely to supersede it in the medium term.. Therefore MSO 2000 format is identified as the emerging standard.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
7: Data interchange (cont.)					
Hypertext interchange formats	Formats for representation and transfer of hypertext documents.	Within CITA scope.	**Primary Standard** HTML v4.01 (Dynamic HTML) Several browser products support this HTML standard. The recognised market leaders are Netscape Navigator v4 and MS Internet Explorer v4. **Secondary Standard(s)** SGML (ISO 8879) for high value, complex publications; XML 1.0 (eXtensible Mark-up Language) (a subset of ISO 8879) where meta-language data definitions are required. WML for constrained environments.	An approved standard for executable content may be required in medium term (eg Java, ActiveX). Monitoring required. XHTML v1.0	The adoption of an approved set of publishing/browser products and a core feature set is required to ensure interoperability. This area is developing particularly quickly hence there is much uncertainty over standards that may emerge in the medium-term. Future use of executable content will be contingent upon the availability of suitable security standards. XML is a standardised text format conforming to ISO 8879, specifically designed for transmitting structured data to Web applications. It addresses the needs of Web publishers who encounter the limitations of HTML to express structured data. It simplifies SGML constructs for electronic delivery of documents and allows structured documents without the full complexity of SGML. Some Web browsers already support XML. More recently XHTML has emerged as a standard. It is a reformulation of HTML v4 in XML v1.0. It is recommended by the W3C and browsers should support it in the near future.
Hypertext transfer protocols	Protocols used for the transfer of hypertext documents.	Within CITA scope.	HTTP v1.1 (RFC 2616).	HTTP with Distribution and Replication Protocol supports the transfer of file differences (deltas) significantly reducing bandwidth consumption. It is reliant upon the use of XML for metadata definitions. HTTP (v2.0), plus executable content-specific protocols in mainstream use at the time. Monitoring is required.	The trend towards executable content means that protocols become content-dependent and are therefore likely to evolve rapidly. This area is developing particularly quickly hence there is much uncertainty over standards that may emerge in the medium-term.

Business-transaction-oriented data interchange standards	Text- or bit-oriented formats for structured representation of business-related data.	Within CITA scope (but limited to those formats employed CCEB-wide).	STEP/ISO 10303 for product data; UN/EDIFACT/ISO 9735 for EDI.	Monitoring required of extent to which formatted messages are in future exchanged between systems in different domains to decide if a CITA standard is necessary in the medium-term. More recently XML has begun to emerge as candidate standard.	The Standard for the Exchange of Product data (STEP), which underpins much of CALS, may ultimately govern much of the information flow with the procurement, management and maintenance of Defence equipment. The use of standards for specific types of CIS is likely to increase (e.g. in Command, Control and Intelligence systems (C2I), and Electronic Data Interchange (EDI) areas) but not all of these are relevant to CITA.
Military data interchange formats	Encodings of military-specific information in structured or unstructured form, including binary (bit-level) encoded and text-based (machine and human- readable) messages.	Within CITA scope.	STANAG 5511: Link 11; STANAG 5516: Link 16,; STANAG 5522: Link 22; OTHT-Gold ADatP3 (STANAG 5500).	Moves towards the use of VMF need to be monitored.	There is an aspiration to employ ADatP3 messages for some inter-nation transfers as interconnections become more widespread. This category does not cover formats related to message handling policy (eg P772) which is covered separately).

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
7: Data interchange (cont)					
Character sets and alphabets	Binary encodings used to represent alphanumeric and special characters.	Within CITA scope.	ITA 5 (ASCII) (International Alphabet #5) 8 bit byte code ISO 8859-1	Monitoring of emergence of acceptably open standards for internationalised character sets required.	Internationalised character sets (e.g. UNICODE/ISO 8859-1) are not yet sufficiently widely adopted to allow their use to be mandated in the current CITA. Such codes should become widely supported and acceptably open in the medium-term, but it is not yet possible to predict which of the potential internationalised codes will dominate.
Encoding standards	Standards for encoding of data, usually for transfer via a communications medium.	Within CITA scope.	**Data Encoding Standards** UUENCODE; MIME; SMIME; zip. **Voice Encoding Standards** ALAW; µLAW (MU-LAW); CELP;	Other encoding standards may be standardised in the context of the interworking services that make use of them (e.g. x.400 or MIME with the standard content encoding types for mail).	This category covers ASN.1 and its encoding rules, BinHex, Base64 etc. UUENCODE converts 8-bit to 7-bit binaries for mail transfer but this function is being superseded by MIME. It is likely that, for many systems, several additional encoding standards will be needed to provide for interoperability with legacy systems. The legacy systems themselves will dictate where and which standards are required. ALAW is a method of companding (or compressing) digitized voice; it is used in Europe and much of the world. µLAW is an alternate method that is used in the United States, Canada and Japan. CELP is a voice coding standard widely used by the military for voice communications over low bandwidth (e.g. 4.8K baud) bearers. Also see data compression standards.

Fax	Standards for transmitting secure an unsecure facsimile between CIS.	Within CITA scope	**Secure Fax** STU-IIB compliant equipment (STANAG 5000 / MIL-STD-188-161D). **Insecure Fax** Group 3 and Group 4;	The use of STE for secure fax and its interoperability with STU-IIB compliant systems needs to be monitored.	The ITU-T Recommendations for Facsimile Standards (Recommendation T.4 (1992) -*Standardisation of Group 3 Facsimile Apparatus for Document Transmission* and Recommendation T.6 (1992) - *Facsimile Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus*) define encoding schemes for black-and-white raster images. Group 3 Fax is now the most widely used fax standard in the world. A Group 3 Body Part is defined for use within X.400. Group 4 Fax is the digital fax standard which is intended in due course to be the replacement for the analogue Group 3 fax. Group 4 may take some time to grow as it requires the use of ISDN.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
7: Data interchange (cont)					
Video Conferencing	Standards for transmitting audio and video between CIS	Within CITA scope	ITU-T H.320, H.221, ITU-T H.224, H.242, H.261, H.230, H.231, H.243, H.233, H.234, H.244;	ITU-T H.323 + ITU-T T.120;	Video conferencing standards are covered by an array of ITU-T H. standards. Proprietary products such as Real Video/Audio by Macromedia Ltd comply with the emerging H.323 and T.120 standards.

Graphical/still image data interchange standards. (Geospatially referenced data formats are dealt with separately).	A wide range of standards used for representation of still image and graphic data, plus fax standards for representation and transfer of page images.	Within CITA scope, Fax standards are dealt with separately.	JPEG v 1.02; GIF v 89a; PNG. Note: Unisys owns a related patent, which requires a licence for software that writes GIF. Readers of GIF have no royalty obligations. National Imagery Transmission Format Standard NITFS 2.1 (MIL-STD 2500B/ STANAG 4545) Note: These two standards are technically the same. NITFS was developed by the National Imagery and Mapping Agency (NIMA). It is used to transmit a file composed of an image accompanied by subimages, symbols, labels, text and other information that relate to the image. One of its main features is that it allows several items of each data type to be included in one file, yet any data types may be omitted. It began as a standard for members of the Intelligence Community, however the NITFS standard has now been accepted within the broader international community. NATO has also adopted this standard and is called NATO Secondary Imagery Format (NSIF) STANAG 4545.	BIIF (ISO 12087 pt. 5) Raster Graphics: ISO/IEC FGC 15444-1 (JPEG2000), ISO/IEC DIS 14495-1 (JPEG-LS) & W3C PNG (Portable Network Graphics) Specification V1.0 (Standardisation of PNG as ISO/IEC 15984) Vector Graphics: W3C WebCGM (Web Computer Graphics Metafile) 1999 & W3CSVG – Scalable Vector Graphics 1.0 Specification (supported in MS Office 2000).	It is likely that, for the majority of systems, several additional standards will need to be supported for interoperability with legacy systems (eg TIFF). Page description standards (eg EPS) are also relevant where images are distributed in an embedded form; these are covered elsewhere. GIF is a non-lossy format for encoding raster images. JPEG is a lossy compressed format which is best for encoding high-resolution photographic images. A JPEG-GIF translation capability is required. This is supported by many mainstream drawing/graphics packages; third-party utilities are also widely available. There is no acceptably open standard for editable graphics. It is assumed that there is no CCEB-wide requirement for standardisation of font representations, nor of specific font designs. In any event, it is evident that there are no acceptably open standards in either of these categories. BIIF (Basic Image Interchange Format), which is based on the National Imagery Transmission Format Standard (NITFS) developed by the US DoD and adopted by NATO, provides a foundation for interoperability in the interchange of imagery and imagery-related data among applications. It provides a detailed description of the overall structure of the format, as well as specification of the valid data content and format for all fields defined within a BIIF file. The BIIF provides a data format container for raster, symbol, and text data, along with a mechanism for including image-related support data.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
7: Data interchange (cont)					

Standard data products/geographic data exchange standards.	This category covers standard data products used within systems and the data exchange standards employed for distribution.	Formats of geospatial and hydrographic data within CITA scope for distribution of standard data products.	The following standard data products/geographic data exchange standards will need to be supported: DIGEST v 2; (all of the other standards conform to this - see notes) S-57 edition 3.	Some rationalisation of formats may be possible. The progress of the OGIS standards needs to be monitored.	There are many GIS in use in existing systems and significant quantities of GIS data in proprietary formats. None of these proprietary formats is sufficiently open to be considered as a CITA standard. Some CITA-conformant systems will need to support additional (proprietary) formats to provide interoperability with specific legacy systems; the legacy systems themselves will dictate where and what additional formats will be needed. In the medium-term, there may be some rationalisation of standards and proprietary formats, reducing the multiplicity of data formats that need to be included within the CITA. Also the Open GIS consortium (OGIS) are attempting to define, among other things, standards for GIS services and data interchange. OGIS is supported by all the main GIS vendors and has the potential to produce acceptably open standard. How far any resultant standards will be adopted and supported is yet to be seen. These developments should be monitored. The recommended geographic data exchange specifications are used as follows: DIGEST is a NATO suite of framework standards for topographic and aeronautical data. S-57 is the International Maritime Organisation standard for hydrographic chart data used for navigational purposes. It has now been harmonised with DIGEST. The recommended standard data products are as follows: DTED is a standard for lat/long-based matrices of terrain elevation data; ASRP is a standard for raster map/air chart data; VMap is a standard for vector map/air chart data. Note that DTED VMap and ASRP are specific standard products conforming to the more general DIGEST specification.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
7: Data interchange (cont)					
Moving image and audio/visual data interchange standards.	A range of standards used for representation of moving images, including standards for video-conferencing and video telephony.	Within CITA scope. There is no identified inter-domain requirement for transfer of moving images or sound, although one may well emerge in the medium-term.	MPEG2 for video (ISO 13818) PCM for Audio (ISO 11172-3) CDFS (ISO 9660).	The commercial market place is rapidly adopting the ITU-H.323 and ITU-T.120 standards for multimedia. These standards together cover all aspects of multimedia (and embody many subsidiary standards). They are used by prominent internet products such as RealAudio and RealVideo.	CDFS is required for interoperability via physical media distribution. The CITA standards are those called up in MIME (RFC 1521 and RFC 1522). These are currently: a. PCM encoding for audio; b. MPEG for video; c. JPEG and GIF for still images (covered under graphical/still image category above). MIME is likely to evolve to support any future standards that become widely adopted, thus the CITA should track evolution of MIME. In particular, although MPEG is the dominant open standard for moving image and audio-visual at the present time, the uptake and status of other standards needs to be monitored. Real Video/Audio are standards proprietary to Macromedia Ltd but appear to be emerging as the dominant standards.
Audio data interchange standards.	As above but for sound. For standards relevant to telephony see section 4.	Within CITA scope.	See moving image and audio/visual data interchange standards above	See moving image and audio/visual data interchange standards above.	Future CITA standardisation of audio is most likely to develop in conjunction with moving image/audio visual standards (see above).
File compression	Standards for encoding/decoding of compact file representations.	Within CITA scope.	zip	Compression standards applied at the application level generally require specific action by end-users to zip and unzip files. General purpose compression applied at lower level (e.g. IP header and payload compression) may provide a more transparent and scaleable service.	The ZIP standard is widely supported by vendors and a variety of platforms. The range of standards requiring support in the medium-term may change.

Multimedia and distributed real time service data interchange standards	All standards under this category are already covered in the Graphics/Still and Moving image categories above.	

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
7: Data interchange (cont)					
Page description	Standards for describing page layouts for submission to print or display devices.	Within CITA scope.	**Primary Standard** PostScript (Level I and Level II); EPS (both proprietary). **Secondary Standard(s)** PDF.	None.	
Miscellaneous data interchange standards	This is a catch-all category of standards not listed elsewhere. It includes: - CASE interchange formats - several page description formats and graphics meta-formats.	. CASE DIF not relevant to interoperability.	N/A	N/A	
8: System and Network Management					
System management	Services supporting the management of end-systems, including user administration, configuration management, fault management, security management, etc.	Outside CITA scope.	None.	None.	Security policy will usually preclude system management interactions between systems, hence there is no need for a CITA standard.
Local Area Network management	Services supporting the management of networks within a nation's local-area communications infrastructure.	Outside CITA scope.	N/A	N/A	LAN management is a purely local issue (ie not relevant to inter-domain interoperability).
National Wide Area Network management	Services supporting the management of networks within a nation's wide-area communications infrastructure	Outside CITA scope.	N/A	N/A	National Wide Area Networks will be managed by national staff hence there is no inter-nation requirement. Also, security policy will usually preclude WAN management interactions between systems. This service area is therefore outside the CITA scope.

Coalition Wide Area Network management	Services supporting the management of the Coalition Wide Area Network (CWAN).	CWAN management at a high level is within CITA scope.	None at present. See note A.19.	None at present.	CWAN management is currently under the control of the Quad C.
Communications bearer system management	Services supporting the management of communications systems forming elements of the CWAN.	Outside CITA scope.	N/A	N/A	Communications systems will be managed by national staff hence there is no inter-nation requirement. Also, security policy will usually preclude management interactions between communications systems. This service area is therefore outside the CITA scope.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
9: Software engineering services	Standards for the system/software lifecycle processes and associated tools plus standards for programming languages and their bindings.	Not relevant to interoperability.	N/A.	N/A.	These services are relevant to porting/reuse of software which can contribute to interoperability in some circumstances; however, there is no significant inter-nation requirement for this.
10: Graphics					
Graphics programming languages and APIs	Languages/language bindings to facilitate the production of graphics-based applications.	Not relevant to interoperability.	N/A.	N/A.	
Application software packages having a drawing capability	Examples include CAD/CAM packages, OA graphics packages.	Not relevant to interoperability.	N/A.	N/A.	OA graphics is covered under Data Interchange.
Military symbology standards	Standards for representation of military symbols (usually on map overlays).	Some relevance to interoperability. (See note.)	MIL-STD-2525B (See note.)	May in future be required to support the exchange of geospatially-referenced data. The requirement for this, in turn, needs to be monitored.	There is currently no requirement to exchange military symbol sets for interoperability. (Requirements for HCI purposes may emerge, but these are not relevant to the CITA). However it is important that the encoding of information is agreed CCEB-wide so that sender and recipient have a common understanding of the data content.
11: Internationalisation	Standards and conventions that facilitate the use or re-use of systems or software within different National or cultural contexts.	Not relevant to interoperability, except character sets which are dealt with under the data interchange category.	N/A	N/A	

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
12a: Messaging security					
Message origin authentication	Service providing assurance that a message was originated by the user indicated as the sender. It is the veritable identification of the user or organisation which originated the message.	CITA should standardise options	ACP 120 (based on X.509 authentication framework).	Inclusion of other authentication services (e.g. higher-level network authentication services) is highly desirable in the medium term subject to maturity and market acceptance of relevant products/ standards.	It is assumed that individual nations will set in place (or defer to) the appropriate organisation to run and administer one or more certification authorities. Certification authorities are an integral part of the X.509 authentication framework. COMPUSEC and COMSEC measures independent of the messaging service can provide lower granularity authentication services (e.g. peer entity authentication provided by key possession where link/packet level encryption is employed).

Message access control	Services for validating authorisation of the user to originate messages is a national prerogative. The originator should ensure that the lowest common clearance of the communications system, end system and recipient dominate the classification of the message. This is to ensure that messages sent do not violate the security policies of the originating domains. Similarly, the receiving domain must compare the classification of the message with the clearance of the receiving domain. For the purposes of interoperability, this only includes standards for exchange of clearance information and security labels.	CITA should standardise: (a) X.411 security label syntax (i.e. the way the labels are represented when they are exchanged); (b) security label semantics (i.e. standardise the meaning of security labels) are currently being specified by the INFOSEC ISME For signatures, see Message Origin Authentication. However, given that, unlike NATO, the CCEB is not a treaty organisation, in the past it has been deemed imposible to take this logical step forward. (c) clearance semantics (i.e. standardise the meaning of clearance attributes) are a subset of the security label and are currently being specified by the INFOSEC ISME. For signatures, see message origin authentication.	Syntax of security labels and clearance attributes are currently being prepared by the Certificate Management Infrastructure Working Group of the INFOSEC ISME.	Apart from security labels, no other access control standards have been identified showing any likelihood of becoming sufficiently widely accepted to permit inclusion within the CITA.	It is assumed that CCEB will define the semantics of security labels exchanged across Defence CIS. The implementation of message access control is usually a local issue; the following functionality is expected of the implementation to support message access control: - in the originator's domain a "CAN SEND CHECK" shall validate the authenticity of the user to send the message (checks his release authority) and that the security label accompanying the message permits the message to leave the originating domain and be received by the intended recipient domain. - message relay and routing a "CAN TRANSFER CHECK" validates that the message can be sent on the next hop, or selects an appropriate route for the message based on the security label accompanying the message - in the recipient's domain "CAN VIEW CHECK" shall validate the authenticity of the user to view (see) the message (that is, the security label accompanying the message permits the message to be seen by the user - ie the user clearance is equal to or exceeds the classification of the message).

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
12a: Messaging security (cont)					
Message content privacy/confidentiality	Services providing confidentiality of message content exchanged between individual end users.	CITA should standardise content confidentiality options.	Based on X.509 authentication framework.	Within the scope of the INFOSEC ISME. However, in the future commercial solutions may be acceptable for meeting the requirements.	Given the requirements to provide adequate COMPUSEC and COMSEC protection throughout the CITA, the underlying confidentiality service will be provided by measures independent of the messaging systems (see general security). It is assumed that, to uphold confidentiality, all application-level message relays will operate system high, multi-level secure or be otherwise trusted. Where content privacy is required it is assumed that CCEB will set up (or defer to) an appropriate organisation to run and administer one or more certification authorities. Certification authorities are a prerequisite of the confidentiality certificate infrastructure.
Message content integrity	Services supporting the integrity of messages exchanged.	CITA should standardise integrity options.	ACP 120 (based on X.509 authentication framework).	None at present. As commercially available security mechanisms and products continue to develop, they may reach a point where the security services they provide are sufficiently strong to meet military requirements.	Integrity is provided by digitally signing a message digest. This in turn relies on X.509 certificates which rely on PKI. It is assumed that individual nations will set in place (or defer to) the appropriate organisation to run and administer one or more certification authorities. Certification authorities are an integral part of the X.509 authentication framework.
Certificate management and distribution	Services supporting the management and distribution of certificates required to implement the message integrity and authentication security services.	Within CITA scope at present, but may be more realistic to be included in future CITA specifications. National policies need to be monitored to determine applicability of commercial standards and Government variants.	X.500 and ACP120 (based on CMI X.509 authentication framework).	None at present. In the future commercial solutions may be acceptable for meeting the above requirements.	Certification authorities are a prerequisite of the authentication certificate infrastructure.

Message non-repudiation with proof of origin	Services providing the recipient of a message with proof of its origin. This provides the ability to prove to a third party that a message was released by the originator and will protect against any attempt by the message originator to falsely deny having sent the message.	CITA should standardise options.	ACP120 (based on digital signatures within the CMI Authentication Framework and associated PKI).	None at present. In the future commercial solutions may be acceptable for meeting these requirements.	Non-repudiation is essentially a security goal that can be achieved using a number of mechanisms. The use of digital signatures with a Public Key Authentication Framework supported by accounting and audit services contribute towards non-repudiation.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
12a: Messaging security (cont)					
Message non-repudiation with proof of delivery	Services providing the originator of a message with proof of its delivery. This provides the ability to prove to a third party that a message was received by a prticular recipient and will protect against any attempt by the message recipient falsely to deny having received the message.	CITA should standardise options.	ACP120 (based on digital signatures within the CMI Authentication Framework and associated PKI).	None at present. In the future commercial solutions may be acceptable for meeting these requirements	See above.
Message security labelling	Services providing a method for associating security labels with objects in a MHS.	See Message Access Control category.	See Message Access Control category.	See Message Access Control category.	
Message accountability	This service provides assurance that messages sent are received by the intended recipient, or permitted alternate recipient. The message originator is notified of any problems with message delivery. This can form a part of overall non-repudiation.	Within CITA scope.	ACP 120 (based on digitally signed receipts and PKI).	None.	Digitally signed receipts are a mechanism for confirming that a message has been received by a specific person or entity. Typically the message recipient will use their private key to sign a hash of the receipt body thus providing the sender with the necessary authentication (of who sent the receipt) and ensuring the integrity of the receipt.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
12b: General security					
Authentication	Services supporting the trusted identification of individual users or groups of users of one system attempting to access services or information provided by another system.	The current CITA should standardise authentication mechanisms in support of secure inter-networking protocols. Inclusion of other authentication services (eg higher-level network authentication services) is highly desirable in the medium term subject to maturity and market acceptance of relevant products/ standards.	None. Awaiting CCEB policy. X.509-based authentication is a possibility. (see note)	Monitoring required of the emergence of strong authentication standards for direct interworking mechanisms. Monitoring also required of the emergence of acceptably open standards for authentication protocols and tokens in support of secure internetworking.	The conclusion regarding the need for secure internetworking protocols is only valid for a limited set of security architectures (i.e. labeled multi-level or compartmented mode systems). It is judged inappropriate for the CITA to restrict the choice of security architecture in this way. Interoperability would nevertheless be enhanced if all systems adopting the above types of security architectures adopt a common authentication protocol. Standard (strong) authentication mechanisms based on the X.509 framework are becoming available and openly standardised for web services. Inclusion of authentication services in the CITA is a prerequisite to many additional interworking services being adopted in the medium term. Authentication (via key possession) will also be promoted via COMSEC measures implemented in the underlying data communications service.
Access control	Services supporting the promulgation of access rights for service/information exchange between systems based on user identity, role, group, clearance or other privilege attributes. This includes standards for security labels where these are used.	The current CITA should standardise security classification labels (i.e. permissible labels and their representation). Standardisation in other areas will be conditional upon a significant shift in the market position of relevant technologies.	None.	Extension of security classification labels to some other emerging CITA interworking mechanisms. Otherwise none at present. Monitoring required of the emergence of strong access control standards for direct interworking mechanisms. Monitoring also required of the emergence of acceptably open standards for authentication protocols and tokens in support of secure inter-networking.	Apart from national standards for security classification labels, no other standards showing a likelihood of becoming widely accepted in the medium-term have been identified. Further standardisation is thus conditional upon a significant shift in the market position of relevant technologies. Access control (via key possession) may also be achieved via COMSEC measures implemented in the data communications service.

Key management and distribution	Services supporting the management and distribution of cryptographic keys.	Outside scope of the current CITA. National policies need to be monitored to determine applicability of commercial standards and Government variants.	None at present.	None at present. The CITA could potentially include key management and distribution schemes for other direct interworking mechanisms.	Key management authorities are a prerequisite of the authentication key management infrastructure.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
12b: General security (cont)					
Data confidentiality	Services supporting the confidentiality of information/services exchanged between systems.	Scope dependent on availability of standards. Confidentiality options within direct interworking mechanisms (e.g. HTTP, RPCs) may be relevant to the medium-term.	Use of ACP 120 application layer data confidentiality or link level encryption.	None at present. There are potential future requirements for data confidentiality options within additional CITA services. Monitoring of the evolution of de facto standards such as S/MIME is required.	Data confidentiality services, to address the threat of direct interception of exposed communications channels, are assumed to be provided as part of the underlying data communications service (e.g. at the link or packet level). Where there is a requirement for confidentiality to be upheld by, for example, an application relay, this must be achieved by appropriately trusted COMPUSEC measures. Requirements for confidentiality options within direct interworking services (ie interworking mechanisms other than messaging) depend on the extent to which these services are themselves adopted in the CITA in the medium term. Traffic flow confidentiality is assumed to be outside scope.
Data integrity	Services supporting the integrity of information/services exchanged between systems.	Scope dependent on the extent to which direct interworking services are adopted in the CITA in the medium term. As for confidentiality above.	Use of ACP 120 application layer digital signatures or link level encryption.	None at present. There are potential future requirements for data integrity options that will support direct CITA interworking mechanisms; however, no applicable open standards can yet be identified. Monitoring required.	Countering the threat of direct attack, data insertion or modification via exposed communications channels is assumed to be addressed by the data integrity services. These can be provided as part of the underlying data communications service or they can operate at the application layer or other layers within the OSI model. Requirements for integrity options within direct interworking services (i.e. interworking mechanisms other than messaging) depend on the extent to which these services are themselves adopted in the CITA in the medium term.

Accounting and audit	Services supporting the recording and analysis of security-relevant events involved in the exchange of services/information between systems.	Within CITA scope. Accounting and audit mechanisms can be used locally to support non-repudiation	CITA may need to adopt the CWAN standards and procedures for accounting and audit. Nations will continue to maintain their own services for accounting and audit.	Requirements for exchange of accountability data between systems to allow audit of distributed applications. Monitoring is required, both of any emerging commercial standards, and of CCEB requirements.	Security is of concern when audit logs are passed through firewalls which typically form the boundary of a system. Management protocols (e.g. SNMP) run over UDP; operating UDP through a firewall will weaken the security it provides.
Non-repudiation	Services to ensure that when information exchange takes place between systems, neither the sender nor the receiver can deny having taken part in it.	Non-repudiation options within information exchange are within scope of the current CITA. However there is currently a lack of standards.	None.	None at present. Monitoring of requirement and standards required.	
Security domain mediation	Services supporting the secure exchange of services between systems operating under differing security policies or within separate security domains (eg firewalls and guards).	Outside scope of the current CITA. A future CCEB-wide security policy may bring such services within CITA scope.	None. Awaiting CCEB policy. Policy should develop to ensure coherent domain mediation through nations' firewalls.	None at present. Monitoring required of emergence of acceptably open standards.	

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
13: Support application software	General-purpose or utility applications software.				
14: Collaborative Computing					
Workflow services	Services supporting the automated transfer of documents or other information between users or organisations on the basis of a predefined business process.	Outside scope of the current CITA. Future inter-nation requirements and the status of emerging standards need to be monitored.	None.	None at present. Monitoring of CCEB requirements for inter-nation exchange of workflow services needs to be monitored.	Acceptably open standards are beginning to emerge (from the Workflow Coalition). They appear, in the main, to focus on the transfer of workflow products between applications. Some applications (e.g. Lotus Notes) are claim compliance with certain API standards.
On line wide-area publishing services.	Services supporting group access (read/write) to structured or unstructured information on the basis of subject area or other categorisation.	Within CITA scope.	**Primary Standard** HTTPv1.1(RFC 2616)/HTMLv4.01. **Secondary Standard(s)** SGML (ISO 8879) for high value, complex publications. XML 1.0 (a subset of ISO 8879) where meta-language data definitions are required.	XHTML v 1.0	.XML was expected to substantially replace HTML as a browser standard. However, more recently XHTML v1.0 has emerged as a candidate. See document interchange.
News group services	Information transfer services designed to notify registered subscribers of updates occurring in newsgroups and transfer relevant information.	Within CITA scope.	NNTP (RFC 977).	None. The evolution of compatible standards needs to be monitored.	
Whiteboarding	Services supporting the sharing of displays across a network allowing multiple users to collaborate simultaneously in the creation, review and updating of graphical or textual information.	Outside CITA scope at present because no firm requirement yet. Possible future requirements and status of standards and products need to be monitored.	None.	Monitoring required of emerging standards (ITU-T T.120 series) and products.(see note).	There are currently no finalised open standards available, though it is to be expected that when the ITU-T T.120 series of standards are agreed, they will be adopted by the industry. Microsoft's data conferencing product Net Meeting is compliant with the communication layer protocols within T.120, however it is not fully compliant with other aspects of the T.120 set. Whiteboarding sessions represent a significant security risk.

Section/category	Summary description	Summary of scope definition	CITA recommendation	Emerging CITA recommendation	Notes
15: Special application software	System- or mission-specific applications software. See note.				Use of identical specialised applications software across systems can contribute to interoperability in some circumstances; however, there is no significant inter-domain requirement for this. Moreover, the extensive and invasive standardisation that would be necessary to support this is not judged feasible. Potential relevance to CITA can only be judged on a case-by-case basis.
GIS	Applications providing a wide variety of services for storing, manipulating and querying geospatial data.	Outside CITA scope (see note).	None.	None.	If a suitable, widely adopted data interchange format emerges then there would be no requirement to standardise on a GIS application (except of application or people portability). The US JTA is silent in regard to recommended applications.
Track Management	Applications providing services relating to the acquisition, correlation, update and query of tracks.	Outside CITA scope (see note).	None.	None.	If a suitable data interchange format emerges then there would be no requirement to standardise.
Alert services	Information transfer services designed to support the rapid or widespread distribution of information, usually having great operational significance.	Outside scope of current CITA because there are no open standards. (see note).	None.	None.	It is deemed desirable for certain alerts to be sent between CCEB nations, particularly in relation to threat warnings. At present, however, there are no open standards and no suitable products.
Data fusion	Services supporting the fusion of data from a variety of possible sources in support of a common opertional picture. See note.	Outside scope of current CITA	None.	None.	It is recognised within the CITA that as coalition forces become more integrated there will inevitably arise the need to fuse data from disparate sources. Such sources of data could be multinational contributing to a truly common operational picture. No standards exist at present hence there is no CITA specification. However it is anticipated that these services could form part of a future CITA.