Allied Data Publication 34

(ADatP-34(D))

NATO Interoperability Standards and Profiles

Volume 5

Rationale for the Selection of NISP Services, Standards, and Technology

Date: 12 January 2010

C3 CCSC NATO Open Systems Working Group

Table of Contents

1. NISP SCOPING PRINCIPLES

1.1. INTRODUCTION

001. This document has been developed and agreed (AC/322(SC/1-WG/4)N(2010)0002-AS1, 24 Mar 10) by the NATO Open Systems Working Group (NOSWG) under the authority of the NATO Consultation, Command and Control Board (NC3B). Under AC/322-N(2010)0038-AS1, the NATO Consultation, Command and Control Board noted ADatP-34(D) and approved the standards and profiles in Volume 2 as mandatory for use in NATO common funded systems in accordance with the NATO networked C3 Interoperability Policy.

002. This document "Rationale for the Selection of NISP Services and Standards" is hereafter known as the Rationale Document (RD).

003. The RD states the process and a set of principles that has been used to govern the scope of technical standardization attempted under the NISP. NATO Common Funded (NCF) Systems will require the standardization of various aspects of Computer Information Systems (CIS) and their supporting Networking and Information Infrastructure (NII). These principles form the first stage of the standards selection rationale process. It is evolving to support the NNEC SOA.

1.2. NISP SCOPING PRINCIPLES

004. The services within the scope of the NISP are derived from the Compendium of NNEC Related Architectures to support the NNEC Networking and Information Infrastructure and the NNEC Capability areas. These services must be scoped for the inclusion in the NISP according to a defined process and set of scoping principles. The NISP has three primary aims:

1. To support interoperability between NCF systems, NII and the national CIS and NII belonging to coalition partners;

2. To deliver benefits to NCF systems by pursuing goals such as application accessibility, people portability and reduced training and through-life cost;

3. To support nation to nation interoperability. This can be achieved using the same boundary services and standards supported at the nation to NCF system and NII boundaries.

005. To support interoperability the NISP must define within its scope a set of services that can reasonably be mandated and supported (within the constraints of security) at the boundary between the systems or infrastructures. For example it is reasonable to mandate that web services should be exchanged using HTTP, but it is unreasonable (and untenable) to mandate that all nations should adopt Windows XP as their operating system or use a common programming language.

006. Consequently the standards specified for each service must be supported at the boundaries. These boundaries are referred to as a Interoperability Point (IOP). National systems may choose

to use other standards internally and translate between the internal and boundary standards. For example, a nation may choose to use bitmap graphics internally but would be mandated to exchange JPEGs at the boundary. The interoperability model is shown diagrammatically below in Figure 1.1.

007. A benefit of this model is that by supporting the boundary services between national and NCF systems, services, and infrastructures, nation-to-nation interoperability will also be supported. Interface Point concepts are described further in NISP volume 1.

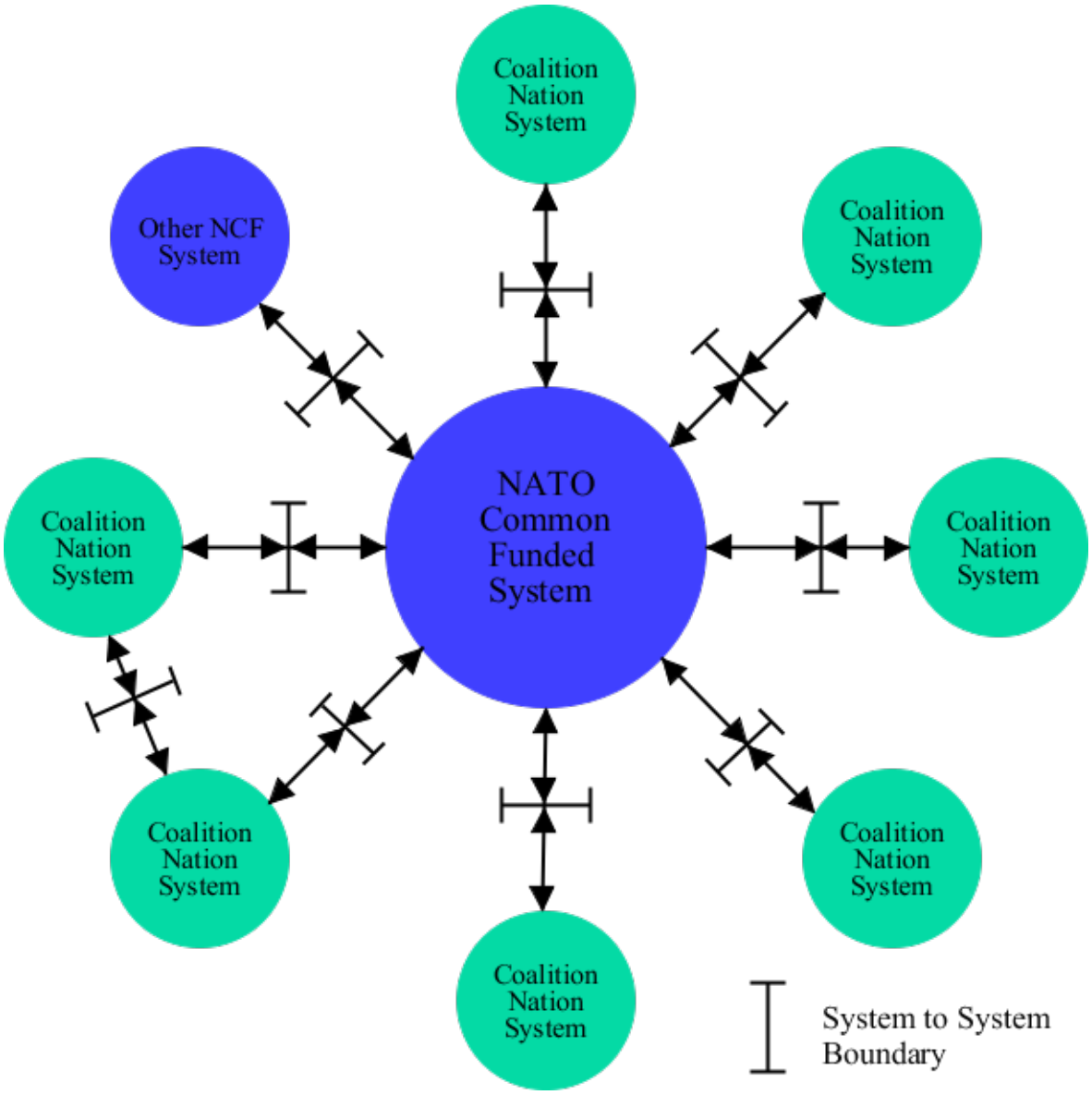

Figure 1.1. Interoperability Model

008. In order to achieve the primary aims of the NISP, the services derived from the NII must be categorized into those that are essential to support:

1. Interoperability at the boundary between systems or NII and must, therefore, be implemented by both coalition nation systems or NII and NCF systems or NII;

2. The wider goals of application accessibility, people flexibility, and reduced training; and

3. Through-life cost for NCF systems.

009. In simple terms, the interoperability services relate mainly to server-server interactions across the boundary between NCF systems or NII and national systems or NII. The NCF system or NII services, however, additionally include both server-server and client-server interactions within NCF systems.

010. Once the services have been categorized, it is then necessary to apply a set of scoping principles that will determine whether a service is within the scope of the NISP. The scoping principles can be subdivided into three groups:

1. A general set of scoping principles that are applied to all services;

2. An interoperability set of scoping principles that are applied to services that are shared between coalition nations, and between coalition nations and NCF Systems;

3. A set of scoping principles that only applies to NCF Systems or NII.

011. A simple flowchart of the process for scoping the services is shown in Figure 1.2. Once the services have been properly scoped into the NISP, the next step is to identify the standards that should be used to implement those services. Suitable justification should be provided as to the reason for each choice of standard.

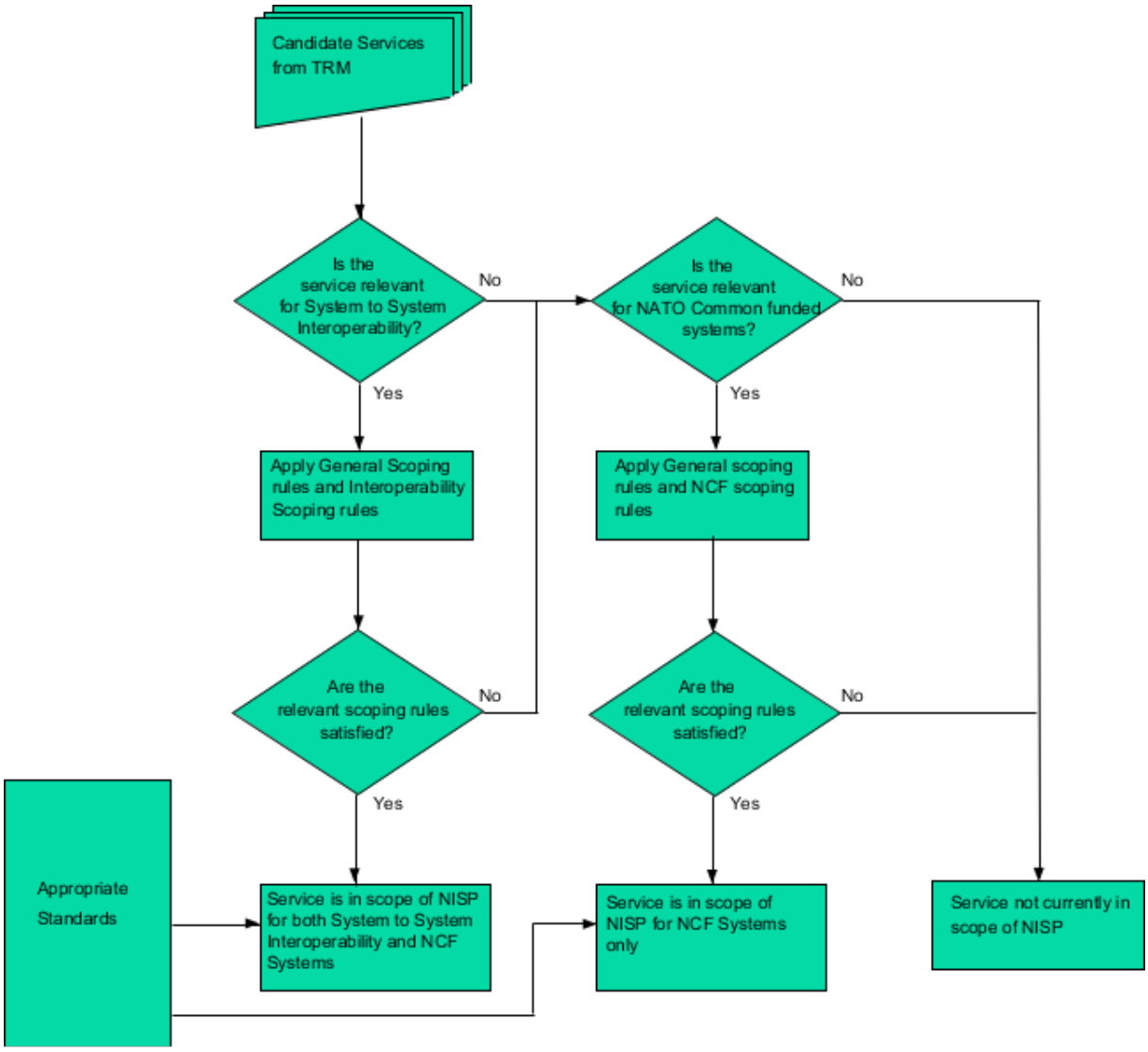

Figure 1.2. Scoping Services

012. The ten key scoping principles are divided into three groups:

- *General scoping principles that are applicable to all candidate services*

  1. Standardization Requirement
  2. Openness
  3. Legacy Issues
  4. Procurement Issues

- *Scoping principles applicable to System to System interoperability candidate services*

5. System boundary issues
6. Interconnection security issues
7. System evolution

- *Scoping principles applicable to NATO Common Funded Systems (NCF) System candidate services (and which are not covered under interoperability)*

8. Application Accessibility/Sharing (guaranteed interoperability by use of the same applications)
9. Reducing life-cycle costs
10. People flexibility and reduced training costs

013. Each of the ten scoping principles are elaborated and explained in the following sections.

1.3. GENERAL SCOPING PRINCIPLES

014. This section defines the general scoping principles that should be applied to all services that are candidates for inclusion in the NISP.

1.3.1. Standardization Requirement

015. For system to system interoperability the NISP should standardize only those services that are relevant to an achievable level of interoperability between NCF systems and between NCF systems and the systems or NII of Coalition partners.

016. There are many NNEC services that are or could be routinely provided within a national NII or an individual system, but which are not relevant to NATO or to a 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 NCF interoperability or System to system's interoperability should be excluded from the scope of the NISP.

017. For NCF systems or NII the NISP should only standardize those services for which there is clear requirement and that would deliver significant benefit when balanced against the reduction in diversity that such standardization would promote.

018. The standardization of services within NCF systems or NII should only be applied when there is a clear need for a particular service. For a service to be standardized, the potential benefits of standardization such as avoidance of vendor lock-in must outweigh the risks of a possible limited market support.

019. The NISP should only standardize services when there is evidence of a present or near term requirement for such standardization.

020. The scope of the NISP, in terms of the services it specifies, will inevitably change over time. There is a temptation to standardize services just in case a future 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 standardization.

021. The NISP should standardize services only where there is sufficient scale of benefit to be gained.

022. There are many standard services that could be potentially beneficial to NCF systems, NII, or in achieving system to system interoperability but their applicability is limited to particular functional niches or the services are needed only by small groups of systems. Unless there is clear benefit from widespread standardization across the NII (with the potential cost and risk penalties of enforcement), the NISP should be silent and the specification of standard services left to a more local level.

1.3.2. Openness

023. The NISP should use only open[1] standards wherever possible when attempting to standardize a service.

024. Products exist that allow IT systems to exchange a wide range of services to achieve a high degree of interoperability; however, some open standards include vendor specific extensions. Therefore it is essential that products be validated against the open standards.

025. Ideally, standardization of a service should only be undertaken where there is an effective open solution. However, there will remain circumstances where effective open solutions do not exist, yet the business benefits of standardization would be significant[2].

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

- There is an effective *de jure* or *de facto* standard. To be effective, there must be wide spread market support for the standard. Among competing standards it should be the dominant standard and it should have a substantial share of the market;

- There is a mainstream product achieving substantial market dominance. Examples of this could be the Microsoft Windows API or the file formats used by the Microsoft Office 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;

[1]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.

[2]One possible example could be office automation; the commercial market has no widely accepted open standards but the business benefits of achieving interoperability in this area are great. In this case the NISP has selected the Microsoft Office formats for interoperability.

- 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.

1.3.3. Legacy Issues

027. Existing standards and profiles implemented in legacy systems should be preferred if they are equal to other candidate standards.

028. There are two reasons why standards already implemented in legacy systems might be preferred: first, they are demonstrated to work and have an experience base; 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 NISP is in essence a forward-looking document that should also indicate the (non-legacy) target standard for migration (embodied later in the system evolution principle) to a more current standard and level of capability.

1.3.4. Procurement Issues

029. For interoperability services, national procurement agencies are encouraged to use the NISP standards, however this should not unacceptably interfere with legitimate national project management or procurement freedoms.

030. The objectives of the NISP require that certain services be standardized across NCF systems and the NII and facilitate interoperability with national NII. However, national projects will need to be individually responsible for specifying national requirements and managing the risks associated with their implementation. NISP standardization aspirations for national systems must therefore be moderated by genuine needs for national project management and control.

031. For NCF systems and the NII the NISP should not standardize services that would interfere with competitive open bidding.

1.4. INTEROPERABILITY SCOPING PRINCIPLES

032. This section defines the scoping principles that should be applied to the services required to support interoperability between NCF systems, the NII and national NII. These principles must be applied in addition to the general principles defined in Section 1.3.

1.4.1. System and Infrastructure Boundary Issues

033. As far as possible, conformance with NISP standards should be confined to requirements to provide specified services at the interface between systems or network infrastructures.

034. For interoperability purposes, the NISP should be confined to specifying those characteristics of systems that are necessary to achieve NCF system interoperability and NCF to coalition nation NII interoperability. It will often be sufficient that systems or networking infrastructures comply with a standard at their external boundaries; interoperability does not necessarily demand that services conforming to the same standards be used internally. Conformance to a standard at the boundary will, however, often mean that certain requirements do need to be satisfied internally. For example, the NISP might demand that a certain external schema is used when relational DBMS information is exchanged; 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.

035. Systems should be capable of meeting NISP external interface standards, but this should not preclude the agreement of additional interfaces between two or more systems if these satisfy local[3] requirements more effectively.

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

1.4.2. Interconnection Security Policy

037. The NISP must embody a practical security policy compatible with the goals of widespread interconnection between systems and NII.

038. Current NATO and Coalition partner security policy guidance regarding the interconnection of secure systems or NII is still being formulated by the NATO Security Committee (NSC). 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 internetworking between NATO and Coalition partner systems or NII.

039. 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 viable security policy within the NISP will be unachievable unless the NATO and Coalition partners can strike a realistic balance between the level of security provided (and thus risk accepted) and the extent of interconnection sought.

[3]In this context 'local' can mean between two CIS or NII from a single nation, internal to NATO or between CIS or NII of different nations.

1.4.3. System Evolution

040. The NISP must accept and provide for a range of standards and technologies to permit interoperability between systems or NII of different technological vintages.

041. Although the NISP will need to evolve in response to technological developments, the pace of evolution of systems or NII will to a large degree depend upon factors outside NISP control (e.g. funding and operational constraints). This means that the NISP must support a range of compatible technologies to support continued interoperability between systems or NII of different NISP 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 NISP must not be delayed too long since this could inhibit end-systems' or NII uptake of those technologies. A balance must therefore be struck between the desire to embrace new technological developments within the NISP and the practical ability of existing systems or NII to evolve to maintain conformance with it.

1.5. NATO COMMON FUNDED SYSTEM SCOPING PRINCIPLES

042. This section defines the scoping principles that should be applied to the services required by NCF systems and NII (other than to support interoperability between NCF systems and NII and national systems and NII). These principles must be applied in addition to the general principles defined in Section 1.3. If any one of these principles provides sufficient benefit the corresponding standards should be adopted.

1.5.1. Application and Service Accessibility

043. For NCF systems and NII it is desirable that the NISP should provide an ability to share common applications and services.

044. Achieving the highest level of interoperability (i.e. guaranteeing that the interpretation and rendering of information is identical within a Community of Interest) frequently depends upon the use of common applications or services (for the same CIS security classification level). Even the best import/export filters can lose or corrupt important elements of information in the process of mapping between formats and encoding standards. In the past application portability was cited as a way of achieving this and deriving benefits from software re-use, but application portability has never been truly realized. However, the ability to have cross-platform availability of applications is achievable by executing applications on a remote server and rendering the display remotely on a user terminal. Hence, in a heterogeneous server environment, users with dissimilar desktops (such as Windows and UNIX) can still access essential applications. The widespread adoption of a Service Oriented Architecture which focuses on the interface, independent of the service implementation, further supports interoperability.

045. Application and service availability also delivers further benefits in the form of reduced training costs (see Section 1.5.3). It also allows the range of different applications and services

to be limited, thus limiting diversity and delivering benefits through the reduction of through-life costs (see Section 1.5.2).

1.5.2. Reducing Life Cycle Costs

046. For NCF systems and the NII it is desirable that the NISP should support an architecture which can embrace technological change and manage obsolescence without the need for radical redesign.

047. The ever-increasing pace of technological development has meant that obsolescence becomes an issue even as systems or services are delivered for the first time. Reducing life cycle costs requires the management of technology obsolescence, which effectively requires key decisions to be made that avoid lock-in or a high dependency on specific products. Systems must be able to evolve in such a way that technology can be refreshed without the need for fundamental redesign.

048. Technology refresh will inevitably increase diversity. An architecture that permits, but manages, diversity will provide a much better environment for the management of obsolescence.

1.5.3. People Flexibility and Training

049. For NCF systems and the NII it is desirable that the NISP should reduce the need for training (and retraining) of personnel in the operation of workstations and applications.

050. Personnel within NATO are required to move within the organisation to execute their role or when changing roles. To make such movements and transfers as efficient and easy as possible it is essential that users are presented with an interface to the services they need that operates and perform in a way that is common across NCF systems and the NII. Adopting a common look and feel through the use of common Human-Computer Interaction (HCI) and style guides will facilitate people portability.

051. Closely linked with people flexibility, there is a need to minimize the amount of training required when personnel transfer between systems. This can best be achieved by adopting a common look and feel to the user interface and adopting a common style guide for application providers.

1.6. AUSTRALIAN AND NEW ZEALAND NATIONAL SUPPLEMENTS TO NISP

052. To further allied interoperability, NATO has also invited the CCEB nations to participate in the NOSWG with the intention that the NISP will be adopted by both NATO and CCEB as the Technical Architecture.

053. If necessary, AS and NZ will develop and publish national supplements to document national variances or exceptions to NISP standards. These instances are expected to be rare.

2. ASSESSMENT OF SCOPE OF NISP

2.1. INTRODUCTION

054. The application of the principles outlined in Chapter 1 has resulted in the assessments captured in the next tables (Table 2.1 to Table 2.4).

Area/ class	Standardization Requirement	Openness	Legacy	Procurement Cost/ risk
1: User Interface Services				
Graphical User Interafce	These services are not necessary for system to system interoperability but do provide benefits to NCF Systems e.g. people portability.training	Standards exist to proliferate User Interface services (e.g. Character-Oriented, Graphical User Interafaces, as well as dedicated) within multiple functional domain areas.	Support is required based on the version of Windows/X Windows utilized.	
Look & Feel	As above	As above	As above	The type of COTS available may be limited in scope or not all-inclusive (e.g. style guides). As a result Military should refer and conform to their respective Defence documents accordingly. Associated costs will differ based on resource applicability.
Toolkit	As above	Toolkits exist to support standards	As above	
2: Data Management				

Area/ Class	Boundary Issues	Interconnection Security Policy	System Evolution	Conclusion
1: User Interface Services				
Graphical User Interafce	N/A	N/A	N/A	Not relevant for system to system interoperability.
Look & Feel	N/A	N/A	N/A	Not relevant for system to system interoperability.
Toolkit	N/A	N/A	N/A	Not relevant for system to system interoperability.
2: Data Management Services				
Dictionary/ Directory	No significant impact.	No significant impact.	No significant impact.	Within NCSP scope.
Database Management System (Relational, Object Oriented)	No significant impact	No significant impact	No significant impact	Within NCSP scope.
Distributed Data	No significant impact	No significant impact	No significant impact	Within NCSP scope.
Remote Data Access	Interworking/middleware products exist which could offer a defined interface at system boundary.	Interconnection security policy will often prohibit direct client/server access between systems.	No significant impact.	In scope of NCSP, however security issues may make system-to-system implementation difficult.
Database Replication	It is generally not feasible to con-	No significant impact	No significant impact	Within NCSP scope.

Area/ Class	Application Accessibility	Reduce In version 4 through-life costs	People Portability and Training	Conclusion
1: User Interface Services				
Graphical User Interafce				Relevant to NCF Systems; remote presentation and IPC are addressed under distributed computing.
Look & Feel				
Toolkit				
2: Data Management Services				
3: Data Interchange				
4: Graphics				
Graphics Programming Languages and APIs				Relevant to NCF Systems for application and people portability
Graphics capability within applications				Relevant to NCF Systems for application and people portability
5: Communications				
6: Operating System Services	Most heterogeneous systems utilize either POSIX or Win 32 Ap-	Linux has emerged as a viable alternative to Unix within		Operating System services are necessary in order to perform

Area/ Class	Definition of class/sub class name	Justification for NCSP Standard Selection
1: User Interface Services		
Graphical User Interafce	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.	Standards are based on the 2 main platforms selected for NATO use: Windows 2000 and Unix. Standards carried forward from NCSP v 2
Look & Feel		Standards are based on the 2 main platforms selected for NATO use: Windows 2000 and Unix. Standards carried forward from NCSP v 2
Toolkit		Standards are based on the 2 main platforms selected for NATO use: Windows 2000 and Unix. Standards carried forward from NCSP v 2
2: Data Management		
Dictionary/ Directory (Data Dictionary)	These are software development support tools that facilitate the management and use of project data dictionaries.	The NC3 Repository is the common repository for standard data elements for the NATO CorpDM. This standard has been selected by the

3. NISP STANDARDS DEFINITION

3.1. INTRODUCTION

055. This section explains the final stage of the NISP definition process, namely the selection and allocation of standards to the services within the scope of the NISP.

3.2. OVERVIEW

056. The process so far has been concerned with the scoping of services from the NII. It has identified those services which are required to support interoperability between NCF systems, the NII, and national systems and NII, and those services that support wider benefits but which can only be mandated for use within NCF systems or the NII. The resultant profile of services (built into a class / sub-class taxonomy) must be implemented using a range of de jure and de facto standards.

057. Among the NII services that are within the scope of the current NISP, there are comparatively few technical choices available for standards that will stand serious scrutiny. This is because the current NISP is limited, for the most part, to those areas where technology is well defined and standards are reasonably stable and well supported. However, it is important that the choice of standards should be justified and to aid this justification a number of key drivers have been used.

3.3. KEY DRIVERS

058. A key driver in the process of selecting the NISP 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 NISP specification has been driven by the following:

1. Adoption of Internet and web technologies. The NISP 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.);

2. Need for security. The most significant departure from commercial standards is in the adoption of a common security protocol particularly in support of messaging. A common approach to secure messaging is fundamental to the existence of an effective NISP;

3. Adoption of essential requirements to meet military needs. Common elements of NATO standards for organizational messaging (STANAG 4406/ACP123) and directory (ACP133) are adopted.

059. The NISP 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 net-work/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.

3.4. MULTIPLE STANDARDS

060. The NISP 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 and 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.

4. NISP EVOLUTION

4.1. INTRODUCTION

061. This section describes the way the NISP will evolve in future issues. It identifies the key change drivers that affect the functionality of systems, the NII and the technology supporting them.

4.2. CHANGE DRIVERS

062. The evolution for the NISP will be driven by the following key factors:

- New technology and its product support in the market place;
- New requirements resulting from the need to interoperate with NATO;
- Resolution of shortfalls in long-term technical issues;
- Feedback from projects and nations implementing the NISP, external stakeholders (e.g. CCEB) and relevant bodies.

4.3. NEW TECHNOLOGY DEVELOPMENTS

063. Close monitoring is required of new technology areas to identify if and when acceptably open, capable standards suitable for NATO and national use become available. These will be addressed in NISP Volume 3, Mid-term Guidance.

4.4. NEW NATO REQUIREMENTS

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

- Overcoming some significant information exchange limitations arising from a lack of acceptably open standards (e.g. Collaborative Computing services);
- Providing NATO-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;
- Standardizing more advanced interoperability mechanisms such as RPCs, other distributed computing mechanisms and database replication services (see Section A.3); these are also contingent on the security developments above;

- Accommodating emerging requirements for the exchange of multimedia-based services between nations.

4.5. FEEDBACK FROM NCF PROJECTS, NATO NATIONS AND OTHER NATIONS AND ORGANIZATIONS

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

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

5. TECHNOLOGY ASSESSMENT METHODOLOGY

5.1. INTRODUCTION

067. To ensure that NATO and its member nations maintain the best use of technology it is important to distinguish between retiring, mandated and emerging technologies/standards. Once they are identified and their applicability analyzed, then informed decisions can be made on what role each technology or standard will play in the current technical architecture.

068. The rapid pace of technological change carries with it the potential benefits of faster and more cost-effective improvements in operational capability; however, the rapidity of change upon a broad technology front also makes the task of identifying emerging technologies particularly difficult.

069. The process of analyzing these emerging technologies will follow 3 steps. The first step is to filter the technologies down to those that are appropriate and applicable to NATO operations. The second step is identifying were in the technology's life cycle are we at the present time. The final step is to describe and forecast the emerging technology's impact on NATO operations.

5.1.1. Filter Criteria

070. The first step in the process of analyzing emerging technologies for NATO is to determine which technologies are relevant to NATO. In other words, we need way to sort through vastly different technologies and focus on only those that influences the answers to the following questions:

- Does it relate to interoperability within NATO Systems?
- Can it effect implementation of NATO CIS?
- Can it effect implementation of NATO Net-Enabled Capability?
- Does it relate to Nation-to-Nation Systems interoperability?

071. So for any given potential technology if we apply any of the above questions and the answer is yes, then that technology has passed the minimum threshold to be a candidate for consideration.

5.1.2. Grading Scale

072. By following 'The Rate of Adoption Theory'[1], we can track the dissemination of a technology over time with innovations going through a slow, gradual growth period, followed by

[1]Rogers, E.M. (1995). Diffusion of innovations (4th ed.). New York: The Free Press

dramatic and rapid growth, and then a gradual stabilization and finally a decline. This model can best track the state of technologies in the IT area of interest.

Phase	**Level**	**Key Attributes**		
		Maturity	**Adoption**	**Support**
Emerging	1	Basic principles observed and reported; Concept and/or applications formulated.	Embraced by early adopters willing to absorb high costs to take advantage of technology	One organization or company controls technology development.
	2	Analytical and experimental critical function and/or characteristic proof of concept.	Embraced by early majority; Common in few NATO nations	Multiple organizations control the technology's development. .
Mandated	3	Component and/or breadboard validation in laboratory and relevant environment.	Internationally widespread and mass market appeal; Common in most NATO nations	Large community involved in the development and improvement of the technology.
Retiring	4	System/subsystem model or prototype demonstra-	Embraced by the conservative	Many advocates, one rival

		tion in relevant & operational environments.	late adopters; Still common, but other alternatives on the horizon.	
	5	Actual system completed and qualified through test and demonstration. Actual system proven through successful mission operations	Better alternatives available.	No advocates, many better alternatives

Table 5.1. ***Key Attributes***

5.1.2.1. Maturity Attribute

073. Technology maturity is a measure of the degree of readiness to which proposed critical technologies meets NATO's objectives. This assessment examines concepts, technology requirements, and demonstrated technology capabilities in order to determine technological maturity. In general,

- Emerging technologies are at a low level of readiness.

- Mandated and retiring technologies have a high level of readiness.

5.1.2.2. Adoption Attribute

074. The adaptation attribute deal with the question of how widespread is the use of a technology. The more ubiquitous a technology becomes, then the lower the costs are for that technology. High rates of adoption also reduce the likelihood of encountering interoperability problems.

5.1.2.3. Supportability Attribute

075. The supportability attribute is a measure of the number of organizations that endorse or supports a technology. More entities involved in developing and sustaining a technology translate into stability.

6. INTEROPERABILITY PROFILE GUIDANCE

6.1. REFERENCES

- (A) NATO Architecure Framework Version 3
- (B) ISO/IEC TR 10000-3:1998(E) Information technology - Framework and taxonomy of International Standardized Profiles - Part 3: Principals and Taxonomy for Open System Environment Profiles

6.2. CONCEPTUAL BACKGROUND

076. ISO/IEC TR 10000 (Ref. B) defines the concept of profiles as a set of one or more base standards and/or International Standardized Profiles, and, where applicable, the identification of chosen classes, conforming subsets, options and parameters of those base standards, or International Standardized Profiles necessary to accomplish a particular function.

077. The NATO Open Systems Working Group (NOSWG) has extended the profile concept to encompass references to NAF architectural views (Ref. A), characteristic protocols, implementation options, technical standards, Service Interoperability Points (SIOP), and related profiles.

078. Nothing in this guidance precludes the referencing of National profiles or profiles developed by non-NATO organizations in the NISP.

6.3. PURPOSE OF INTEROPERABILITY PROFILES

079. Interoperability Profiles aggregate references to the characteristics of other profiles types to provide a consolidated perspective.

080. Interoperability Profiles identify essential profile elements including Capability Requirements and other NAF architectural views (Ref. B), characteristic protocols, implementation options, technical standards, Service Interoperability Points, and the relationship with other profiles such as the system profile to which an application belongs. Interoperability profiles will be incorporated in the NATO Interoperability Standards and Profiles (NISP) for a specified NATO Common Funded System or Capability Package to include descriptions of interfaces to National Systems where appropriate.

081. NATO and Nations use profiles to ensure that all organizations will architect, invest, and implement capabilities in a coordinated way that ensure interoperability for NATO and the Nations. Interoperability Profiles will provide context and assist or guide information technologists with an approach for building interoperable systems and services to meet required capabilities.

6.4. APPLICABILITY

082. Since the NISP impacts on the full NATO project life cycle, NISP stakeholders may include engineers, designers, technical project managers, procurement staff, architects and other plan-

ners. Architectures, which identify the components of systems operation, are most applicable during the development phase of a project, when applied to the dynamic NNEC environment, where interoperability of mature National systems requires an agile approach to architectures.

083. The NOSWG has undertaken the development of interoperability profiles in order to meet the need for specific guidance at interoperability points between NATO and Nations systems and services required for specific capabilities. As a component of the NISP, profiles have great utility in providing context and interoperability specifications for using mature and evolving systems during exercises, pre-deployment or operations. Application of these profiles also provides benefit to Nations and promotes maximum opportunities for interoperability with NATO common funded systems as well as national to national systems. Profiles for system or service development and operational use within a mission area enable Nations enhanced readiness and availability in support of NATO operations.

6.5. GUIDELINES FOR INTEROPERABILITY PROFILE DEVELOPMENT

084. Due to the dynamic nature of NATO operations, the complex Command and Control structure, and the diversity of Nations and Communities of Interest (COI), interoperability must be anchored at critical points where information and data exchange between entities exists. The key drivers for defining a baseline set of interoperability profiles include:

- Identify the Service Interoperability Points and define the Service Interface Profiles
- Use standards based consistent with the common overarching and reference architectures
- Develop specifications that are service oriented and independent of the technology implemented in National systems where practical
- Use mature technologies available within the NATO Information Enterprise
- Develop modular profiles that are reusable in future missions or capability areas
- Use an open system approach to embrace emerging technologies

085. The starting point for development of a profile is to clearly define the Service Interoperability Point where two entities will interface and the standards in use by the relevant systems.

086. The use of "shall" in this guidance document is intended to establish a minimum level of content for NATO and NATO candidate profiles, but is suggested-but-not-binding on non-NATO profiles (national, NGO, commercial and other entities).

087. The NISP is the governing authoritative reference for NATO interoperability profiles. DOTMLPFI capability analysis may result in a profile developer determining that some of the capability elements may not be relevant for a particular profile. In such cases, the 'not applicable' sections may either be marked 'not applicable' or omitted at the author's discretion.

6.6. PROFILE TAXONOMY

088. The objective of the interoperability profile taxonomy is to provide a classification scheme that can categorize any profile. In order to achieve this objective, the classification scheme is based on NATO Architecture Framework views and DOTMLPFI characteristics.

089. The taxonomy illustrated in the figure below will also provide a mechanism to create short character strings, used as a root mnemonic to uniquely identify profiles.

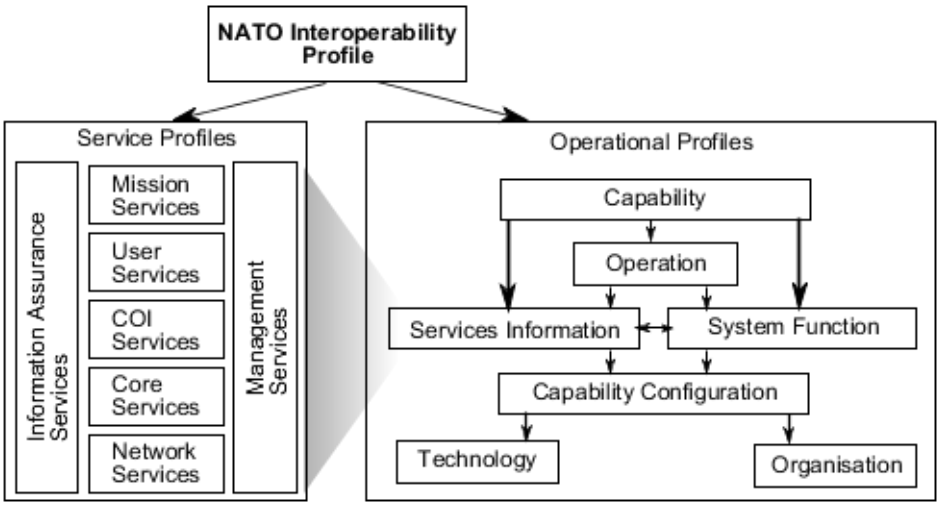

Figure 6.1. Interoperability Profile Taxonomy

6.7. STRUCTURE OF INTEROPERABILITY PROFILE DOCUMENTATION

090. This section identifies typical elements of Interoperability Profile Documentation.

6.7.1. Identification

091. Each NATO or candidate NATO Interoperability Profile **shall** have a unique identifier assigned to it when accepted for inclusion in the NISP. This **shall** be an alpha-numeric string appended to the root mnemonic from the NISP profile taxonomy.

6.7.2. Profile Elements

092. Profile elements provide a coherent set of descriptive inter-related information to NATO, national, NGO, commercial and other entities ('actors') desiring to establish interoperability.

093. Profiles are not concepts, policies, requirements, architectures, patterns, design rules, or standards. Profiles provide context for a specific set of conditions related to the aforementioned documents in order to provide guidance on development of systems, services, or even applica-

tions that must consider all of these capability related products. Interoperability Profiles provide the contextual relationship for the correlation of these products in order to ensure interoperability is 'built-in' rather than considered as an 'after-thought'.

6.7.2.1. Capabilities Set

094. Each profile **shall** list the Capabilities supported by the profile. The intention of this section is to trace NATO capabilities to the applicable element(s) in the NATO capability taxonomy/database and NNEC Maturity Level (NML), as well as any relevant authoritative capabilities operational reference documents (e.g., Overarching Architecture, EXTAC reference, etc.). Identification of applicable functional attributes is desired to link capability requirements to objective or subjective interoperability performance objectives.

Table 6.1. Capability Set Taxonomy, Reference and Applicable Functional Attributes

Related Capability Title	High-level Capability Description (extract from NATO Capabilities Database)	NML Ref #	NATO Capability Taxonomy Ref. #	Reference (Overarching Architecture, EXTAC, etc.)	Applicable Functional Attribute(s)

095. Each profile should list the Functional Attributes supported by the profile. The intention of this section is to identify what functional attributes are desired and thus link capability requirements to interoperability performance thresholds and objectives. For example, a typical threshold for satisfactory equipment performance may be achieving 95% reliability calculated in accordance with a specified military standard such as MIL-HDBK-217F(2) 'RELIABILITY PREDICTION OF ELECTRONIC EQUIPMENT'.

Table 6.2. Functional Attributes**

Functional Attribute	Threshold/ (for minimum satisfactory performance)	Objective
Superior Decision Making		
Flexible Synchronization		
Shared Understanding		
Responsible and Adaptable Organization		
Dispersed C2		
Simultaneous C2 Processes		
Full Spectrum Integration		
Shared Quality Information		
Robust Networking		
TBD		

096. ** 'notional' Attributes shown in the table above are for illustrative purposes only.

097. Each profile should document the relationship between Capabilities and Operational Activities supported by the specific interoperability profile. The intention of this section is to map capabilities to operational activities thereby providing implementation authorities with vital un-

derstanding as to what actors will be establishing what NML is being sought at specific Service Interoperability Points (SIOPS). Identification of entities may be generic, specific, or a combination of generic and specific entities. For example, it may be unrealistic and inappropriate to identify specific operational units, deployable headquarters, and/or non-NATO actors for a reference-architecture (high-level) profile. However, specific identification of operational activities may be totally appropriate for developing a target-level profile associated with promoting interoperability for a specific discrete event or set of events in theatre.

Table 6.3. Capability to Operational Activities Mapping

Related Capability/ Title	Operational Activity	Requirement Reference	Cross Reference

6.7.2.2. Applicable Standards

098. Each profile **shall** document the standards required to support this or other associated profiles and any implementation specific options. The intention of this section is to provide an archive that shows the linkage between evolving sets of standards and specific profile revisions.

Table 6.4. Applicable Standards

Profile ID	**Mandatory Standards**	**Emerging Standards**	**Implementation Options**			
A unique profile identifier	A unique Standard Identifier from the NISP	A unique Standard Identifier from the NISP	Implementation specific options associated with this profile (may be a reference to a separate annex or document)			

6.7.2.3. Related Profiles

099. Each profile should document other key related system or service profiles in a cross reference table. The intention of this section is to promote smart configuration management by including elements from other profiles rather than duplicating them in part or in whole within this profile. Related profiles would likely be referenced in another section of the profile.

Table 6.5. Related Profiles

Profile ID	Profile Description	Community of Interest	Associated SIOPs
A unique profile identifier	A short description of the profile	Air, Land, Maritime, Special Ops, etc.	Unique SIOP identifiers

6.7.2.4. Services Mapping

6.7.2.4.1. Capability / Function / Service Mapping

100. Each profile should provide a cross reference between Capabilities, System Functions and Services. The intention of this section is to specify 'services mapping' both for stakeholders with relevant service-oriented architectures (SOAs), and for interoperability within multi-entity federated environments where functional information may be relied upon as a key information source or 'service'. The services mapping is vital to illustrating the sometimes complex interoperability interrelationships among services, system functions and operational capabilities.

Table 6.6. Capability-to-Function-to-Service Mapping

Service ID #	Supported Capability Title (from table 1)	System Function (from table 17)	Service/(from tables 7 and 8)

6.7.2.4.2. Capability Specific COI Services

101. Each profile **shall** describe any known COI services required to support the profile. The intention of this section is to specify those services for which reuse in other capability areas would be the exception rather than the rule. For example, if one developed a service for developing Air Tasking Orders (ATOs) in support of Air Command and Control, this would be a COI-specific service.

Table 6.7. COI Services Description (capability-specific)

ID #	COI Service (capability-specific)	Service Definition Description

6.7.2.4.3. Cross COI Service Re-use

102. Each profile should describe any other COI services being reused to support this profile. The intention of this section is to specify those services for which reuse in other capability areas is expected or likely. For example, geospatial display capabilities would be useful in support of a variety of capabilities, and thus should be listed in this Cross COI / Service Re-use section of the profile.

Table 6.8. COI Services (cross-COI / re-use)

ID #	COI Service (cross-COI / re-use)	Service Definition / Description

6.7.2.4.4. Service Related Capability Specific Constraints

103. Each profile should describe any service related capability constraints, such as Quality of Service (QoS). The intention of this section is to identify Quality of Service (QoS) requirements and related constraints. QoS is often vital to establishing viable interoperability. Interoperability is of limited or questionable value if the information does not meet the expectations of the actors/entities on the other side of the Service Interoperability Point (SIOP). Identification of constraints is intended to supplement the Quality of Service definitions by adding to the understanding of factors that may limit interoperability QoS on either or both sides of the SIOP (e.g., available bandwidth, format restrictions, circuit limitations, etc.).

104. NOTE: Information Assurance (IA) constraints have been intentionally omitted from this revision of profile guidance with the view that IA features will be embedded in the architectures and tend not to be a capability-specific concern. However, if capability-specific IA functionality is required, it may be appropriate to include IA-specific constraints in this section, or to insert a separate IA section.

Table 6.9. Service-related capability-specific constraints

ID #	Constraint	Description	Reference

6.7.2.5. Key Operational Definitions

105. Each profile should list relevant agreed operational definitions within the scope of the profile. The intention of this section is to promote a common understanding of the operational terms used across interfaces among different entities (i.e., semantic interoperability). For example, for

an MSA profile, one may provide a specific definition for the term 'vessel of interest' in order that the term may be properly understood and/or translated across the interface.

Table 6.10. Key Operational Definitions (semantic vocabulary)

Abbreviation (if any)	Term	Definition	Reference

6.7.2.6. Operational Concepts Descriptions

106. Each profile should list the operational concepts within the scope of the profile. The intention of this section is to identify operational concepts that provide relevant context for implementation authorities to understand how interoperability will enable and support achieving mission success. 'DOTMLPFI' categories refer to considering interoperability within the context of delivering comprehensive capabilities to operational users. 'DOTMLPFI' is an acronym that means 'Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and Interoperability'. Some of these elements may not be applicable. The use of the

term DOTMLPFI is not intended to be exhaustive or exclusive. Thus, other capability elements such as policy and legal may be added as deemed appropriate.

Table 6.11. Key Operational Definitions (semantic vocabulary)

Operational Concept	Categories (DOTMLPFI, policy, legal, etc.)	Classification	Reference	Originating Organization

6.7.2.7. Operational Node Connectivity Description

107. Each profile should provide a diagram of the operational nodes connectivity supported by this profile. The intention of this section is to identify operational nodes to provide implementation authorities with a more detailed description of the required/desired interoperability end state (i.e., goal baseline) connectivity. Identification of operational nodes may be generic, specific, or a combination of generic and specific elements.

[Insert Notional Node Connectivity Diagram/Figure from NOV-2]

Figure 6.2. Notional Node Connectivity Diagram

108. Each profile should describe the contribution and connectivity of each operational node supported by the profile. The intention of this section is to support the development or use of NOV-2 or NOV-2-like architecture view(s).

Table 6.12. Operational Node Connectivity Description (NOV-2 precursor)

Operational Node	Contribution(s)	Connectivity Description

6.7.2.8. Operational Information Requirements

109. Each profile should list the relevant operational information requirements (preferably described using APP-15) within the scope of the profile. This section is intended to promote the NNEC need to share information in a Service Oriented Architecture by documenting Information Requirements associated with this profile to support the NATO Data Strategy making data visible, accessible and understandable. If such information is maintained in an external document, reference to such documentation is preferred - including the most recent revision associated with this particular profile baseline.

Table 6.13. Operational Information Sharing Matrix (NOV-3 precursor)

IER/#	X x #	Event Action	Information Characterisation	Receving Node	Critical	Format	Timeliness	Classification	Cross Reference
				(Command, Etc.)	Yes No	Text Data Audio Video Voice	(eg. less than 15 Sec.)	NU NR NS	

6.7.2.9. Criteria of Operational Interest

110. Each profile should list relevant key conformance criteria of operational interest. The intention of this section is to document criteria such as alerts, thresholds or other parameters that may be important to understanding and employing information shared across an interface. This list of key criteria is not intended to be exhaustive. Additionally, if such criteria are described in a separate document referencing the document is appropriate. For the sake of brevity, it is highly encouraged to reference (not duplicate) other documents when completing this section.

Table 6.14. Criteria of Operational Interest

ID #	Key Criteria of Operational Interest	Definition / Description

6.7.2.10. Capability Configuration

111. Each profile should describe the capability baseline that the profile supports. The intention of this section is to identify "as is" capability baselines that have used this profile. Since profiles tend to evolve, the specific profile revision used to achieve interoperability is also noted.

Table 6.15. Capability Configuration

Capability Baseline #	Date (YYYYMM-DD)	Name of Capability Baseline and Originator	Profile(s) / Revision Used/(High Level Overview / Synopsis)

6.7.2.11. Organizational Interfaces

112. Each profile **shall** include a description of the organizational interfaces supported by the profile. The intention of this section is to promote visibility and interactions among stakeholders. Note that the intention of this section is very different than the aim of the Operational Node Connectivity Description. This section is intended to be more administrative in nature

and identify stakeholders and contributors to the profile. Generic organizational billets and/or specific points of contact may be identified in this section as desired.

Table 6.16. Organizational Interfaces

Organization (Short Title)	List of Required Organizational Interfaces	Detailed Notes regarding Organizational Interfaces

6.7.2.12. System Functions

113. Each profile should list the system functions that the profile supports. The intention of this section is to provide a basic understanding of the system functional decomposition on the profile implementation authority's side of the SIOP. The intent of this section is to make the profile less abstract and more concrete for the implementation authorities on both sides of the SIOP as they work to achieve interoperability. There is no intention of renaming functions on the other side of the SIOP, but rather to provide insight regarding what functions will be supported by

information crossing the SIOP interface(s). Detailed system functional descriptions should be cited as references, not duplicated.

Table 6.17. System Functions and Descriptions

ID #	System Function	Function Definition/Description

6.7.2.13. Candidate Technologies

114. Each profile should document the current and emerging technologies required to support this profile and any implementation specific options. The intention of this section to identify current and emerging technologies associated with promoting interoperability as an aid to stakeholder organization program managers as they consider (with interoperability in mind) their own mid-term (2-6 years) and long term (>6 years) investment plans in relevant technologies.

Technology ID	Current Technologies	Current Technologies	Current Technologies	Implementation Options
A unique technology identifier	Technology name(s)			Implementation specific options associated with this profile (may be a reference to a separate annex or document)

Table 6.18. Candidate Technologies

6.8. VERIFICATION AND CONFORMANCE

115. Each profile **shall** identify authoritative measures to determine verification and conformance with agreed quality assurance, Key Performance Indicators (KPIs), and Quality of Service standards such that actors are satisfied they achieve adequate performance.

116. Stakeholders are invited to provide feedback to improve a profile's verification and conformance criteria.

117. Verification and Conformance is considered in terms of the following five aspects:

1. Approach to Validating Service Interoperability Points

2. Relevant NNEC Maturity Level (NML) Criteria

3. Key Performance Indicators (KPIs)

4. Experimentation

5. Demonstration

6.8.1. Approach to Validating Service Interoperability Points

118. Each profile should describe the validation approach used to demonstrate the supporting service interoperability points. The intention of this section is to describe a high-level approach or methodology by which stakeholders may validate interoperability across the SIOP(s).

6.8.2. Relevant NNEC Maturity Level (NML) Criteria

119. Each profile should describe the NML criteria applicable to the profile. The intention of this section is to describe how this profile supports the achievement of improved interoperability within the NML framework.

6.8.3. Key Performance Indicators {KPIs)

120. Each profile should describe the associated Key Performance Indicators (KPIs) to establish a baseline set of critical core capability components required to achieve the enhanced interoperability supported by this profile. The intention of this section is to assist all stakeholders and authorities to focus on the most critical performance-related items throughout the capability development process.

Table 6.19. Key Performance Indicators {KPIs)*

Key Performance Indicators (KPI)	Description
KPI#1: Single (named) Architecture	
KPI#2: Shared Situational Awareness	
KPI #3: Enhanced C2	
KPI #4: Information Assurance	
KPI #5: Interoperability	
KPI #6: Quality of Service	
KPI #7: TBD	

121. *'notional' KPIs shown in the table are for illustrative purposes only

6.8.4. Experimentation

122. Each profile should document experimentation venues and schedules that will be used to determine conformance. The intention of this section is to describe how experimentation will be used to validate conformance.

6.8.5. Demonstration

123. Each profile should document demonstration venues and schedules that demonstrate conformance. The intention of this section is to describe how demonstration will be used to validate conformance.

6.9. CONFIGURATION MANAGEMENT AND GOVERNANCE

6.9.1. Configuration Management

124. Each profile **shall** identify the current approach or approaches toward configuration management (CM) of core documentation used to specify interoperability at the Service Interoperability Point. The intention of this section is to provide a short description of how often documents associated with this profile may be expected to change, and related governance measures that are in place to monitor such changes [e.g., the NOSWG].

6.9.2. Governance

125. Each profile **shall** identify **one or more authorities** to provide feedback and when necessary, Request for Change Proposals (RFCP) for the Profile in order to ensure inclusion of the most up-to-date details in the NISP. The intention of this section is to provide a clear standardized methodology by which stakeholders may submit recommended changes to this profile.

6.10. DEFINITIONS

Table 6.20. Definitions

Term	Acronym	Description	Reference

6.11. ANNEX DESCRIPTIONS

126. The following describes a list of potential **optional** annexes to be used as needed. The intention of this section is to place all classified and most lengthy information in Annexes so that the main document stays as short as possible. In cases where tables in the main document become quite lengthy, authors may opt to place these tables in Annex D.

127. Annex A - Classified Annex (use only if necessary)

128. Annex A-1 - Profile elements (classified subset)

129. Annex A-2 - (Related) Capability Shortfalls

130. Annex A-3 - (Related) Requirements (classified subset)

131. Annex A-4 - (Related) Force Goals

132. Annex A-5 - other relevant classified content

133. Annex B - Related Architecture Views (most recent)

134. Annex B-1 - Capability Views (NCV)

- NCV-1, Capability Vision
- NCV-2, Capability Taxonomy
- NCV-4, Capability Dependencies
- NCV-5, Capability to Organisational Deployment Mapping
- NCV-6, Capability to Operational Activities Mapping
- NCV-7, Capability to Services Mapping

135. Annex B-2 - Operational Views (NOV)

- NOV-1, High-Level Operational Concept Description
- NOV-2, Operational Node Connectivity Description
- NOV-3, Operational Information Requirements

136. Annex B-3 - Service Views (NSOV)

- NSOV-1, Service Taxonomy
- NSOV-2, Service Definitions (Reference from NAR)
- NSOV-3, Services to Operational Activities Mapping (in conjunction with NCV-5, NCV-6, NCV-7, NSV-5 and NSV-12)
- Quality of Services metrics for the profiled services

137. Annex B-4 - System Views (NSV)

- NSV-1, System Interface Description (used to identify Service Interoperability Point (SIOP))
- NSV-2, Systems Communication DescriptionNSV-2d, Systems Communication Quality Requirements

- NSV-3, Systems to Systems Matrix
- NSV-5, Systems Function to Operational Activity Traceability Matrix
- NSV-7, System Quality Requirements Description
- NSV-12, Service Provision

138. Annex B-5 - Technical Views (NTV)

- NTV-1, Technical Standards Profile. Chapter 4 of the NAF Ref (B) provides more specific guidance.
- NTV-3, Standard Configurations

139. Annex C - Program / Inter-Programme Plans

140. Annex C-1 - (Related) Mid-Term Plan excerpt(s)

141. Annex C-2 - (Related) Programme Plan excerpt(s)

142. Annex D - Other Relevant Supporting Information

This page is intentionally left blank

A. NISP RATIONALE DOCUMENT - SUPPLEMENTARY INFORMATION

A.1. INTRODUCTION

143. This annex provides additional explanatory material in support of the standards assessment in the Rationale Document.

A.2. ENTERPRISE-LEVEL DATA MANAGEMENT

144. 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.

145. There are other reasons why more extensive standardisation of data might be advantageous (e.g. application portability) and these concerns are relevant to NCF systems.

146. 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.

147. 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 NATO-wide agreements, encapsulated within the NISP.

148. These issues, and the wider role of data management within NATO must be reviewed. The eventual scope and form of the NISP will therefore be influenced by this work.

149. 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 NISP, and to pre-determine the nature of requests for information exchange.

A.3. DATABASE TO DATABASE REPLICATION

150. 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 area are the more sophisticated protocols employed within commercial products capable of transaction management, selective attribute-based replication, etc.

151. 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 an NCOE standard but no product currently has sufficient market dominance to justify this.

A.4. OA INTERCHANGE FORMATS

152. *De jure*document interchange standards have neither the richness nor the product support to be credible interchange standards. (An exception to this is XML, a specific application of SGML, which is considered under a separate class.) 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.

153. 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.5. HYPERTEXT INTERCHANGE FORMATS

154. The requirement for document interchange can be satisfied to a degree by the adoption of hypertext formats (and other mark-up formats such as XML) 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. With the widespread adoption of XML (and XSL) the functionality gaps are narrowing.

A.6. MESSAGING

155. The X.400 functional model and a typical client/server messaging configuration are shown in Figure A.1.

156. 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. These often include Groupware functionality as well as messaging functionality that would force many systems adopting X.400-compliant MS and UA products to provide more mainstream products.

157. 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.

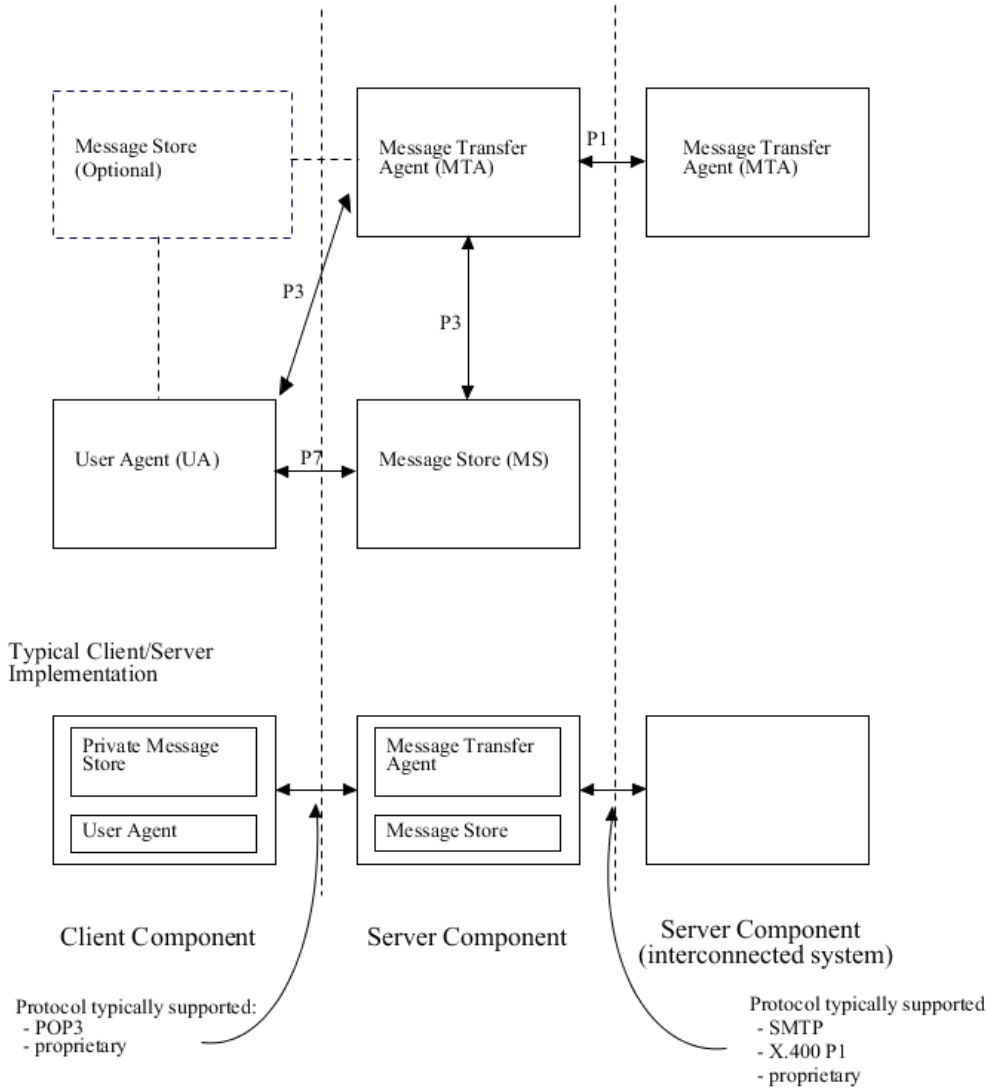

Figure A.1. X.400 Functional Model

A.7. DIRECTORY

158. Projects' selection of a directory product is usually dictated by their choice of messaging product (e.g. Microsoft Exchange requires the use of Active Directory in order to provide a messaging service). However, X.500-compliant products (as required by NATO) are commercially available, and are becoming more de-coupled from the messaging service. Meta-directories now offer a viable solution to the integration of different directory products. LDAP v3 is the internationally accepted access protocol supported by all vendors.

A.8. KEY MANAGEMENT AND DISTRIBUTION

159. Few 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 little possibility of standardising an asymmetric key distribution service within the NISP (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).

160. Clearly, however, if widespread use is to be made of cryptographically-delivered security services within other NISP services (notably messaging), there will ultimately be a requirement to standardise key distribution services. Progress on this front within the NISP is contingent upon current NATO security architecture work.

A.9. SYSTEM MANAGEMENT

161. This area 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]

162. With an ever-increasing level of integration between NATO and national 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 amongst allies and coalition partners.

A.10. NETWORK MANAGEMENT

163. This area is taken to mean the exchange of management information and services among end-systems and between end-systems and the wide-area communications infrastructure in order to permit remote network management or the simultaneous management of several systems' local network components. Strong local network management control is therefore usually required to enforce local system security policies.

A.11. NAME SERVICES

164. 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 used to support secure messaging.

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

A.12. OBJECT INTERCHANGE

165. 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 opestandards. Most use remote procedure call (RPC) mechanisms to effect distribution of computational effort, the exception being Java The main contendees are:

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

- 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.

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

- 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.

- SOAP: is a W3C, XML-based, commercially supported protocol that is widely adopted. Unlike the currently mandated standards (CORBA & COM) it uses an open transport mechanisms (e.g. HTTP) which is mandated in the NISP.

A.13. ALERT SERVICES

166. 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 all-informed or multicast basis and, on efficieny 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.

167. Requirements for alerts arise in two ways in NATO CIS:

- for distribution of urgent system management messages or instructions;

- for rapid dissemination of operationally significant information such as warnings.

A.14. ARCHITECTURAL CONCEPTS

168. The NISP is predominately based upon the concept of a federation of fixed and mobile systems that together form a NATO Intranet. Embodied within the NISP, 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;

169. Other mandated applications, however, (e.g. X.400 messaging) have been designed to use the seven-layer OSI protocol stack (see Figure A.2) which has the following seven layers:

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

170. These two protocol stacks align as shown in Figure A.2. Their use creates a dichotomy in the NISP that requires ISO transport services to be layered on top of TCP/IP (as defined in RFC 1006).

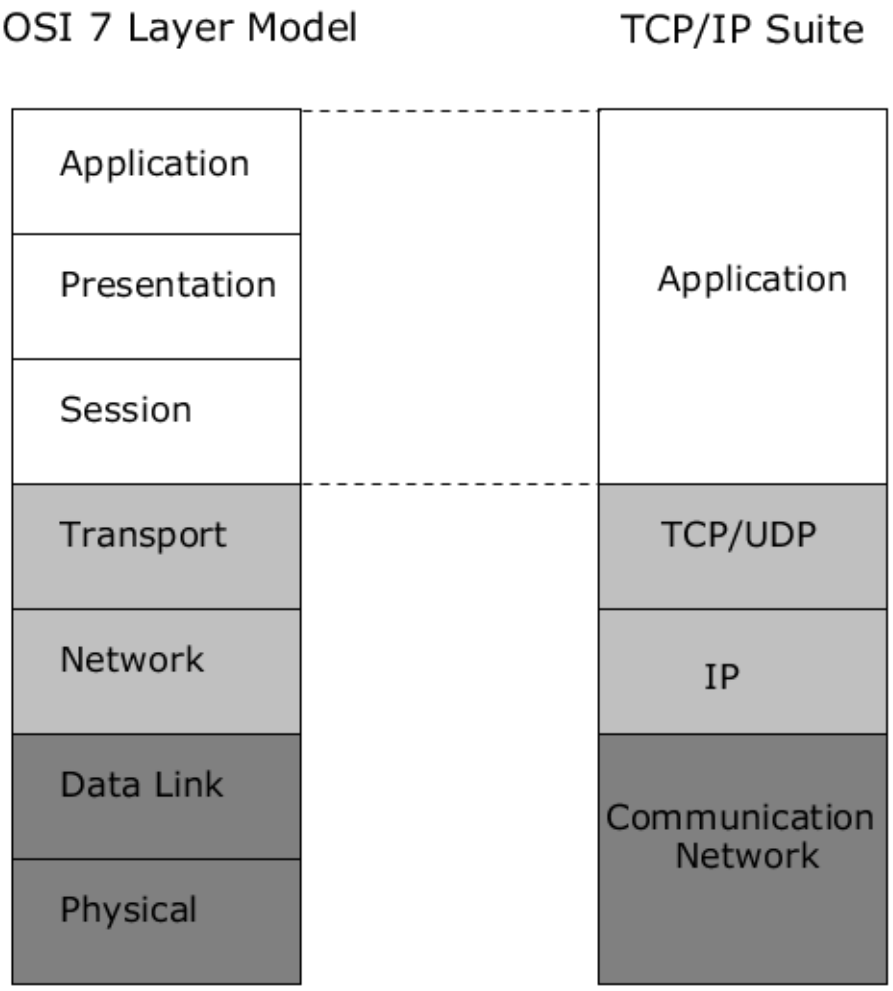

Figure A.2. OSI and TCP/IP Protocol Stacks

171. Both of these stacks are embodied in the NISP, although their purpose may not be immediately obvious, so that ISO-based applications such as X.400 and X.500 can be supported as illustrated in Figure A.3.

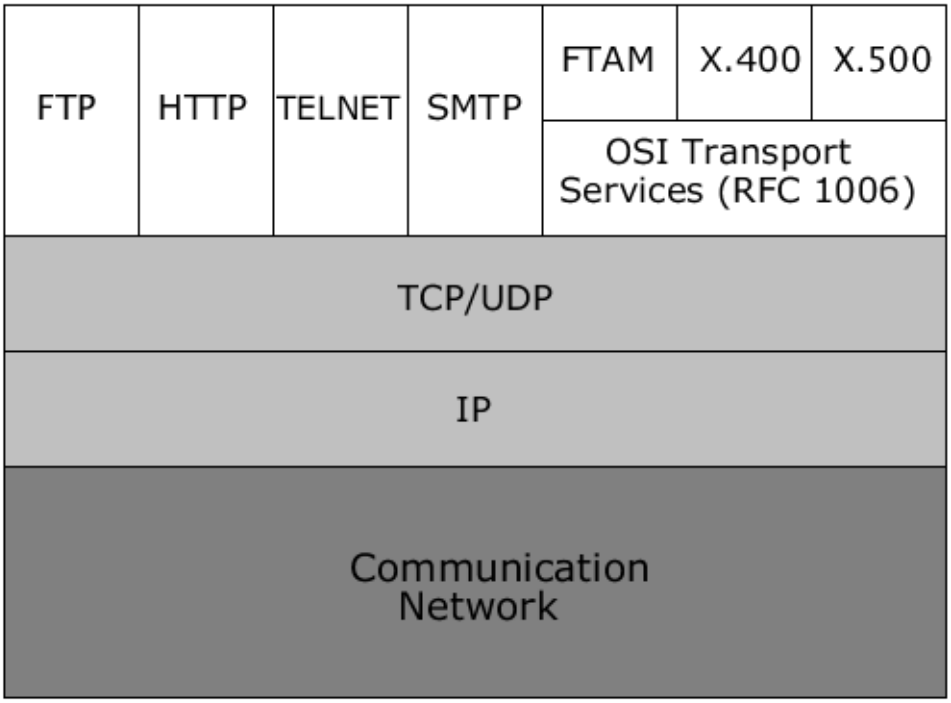

Figure A.3. OSI and TCP/IP Applications

A.15. COALITION WIDE AREA NETWORK (CWAN) MANAGEMENT

172. 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.15.1. CCCC Management Overview

173. 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.

174. 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 cen-

ter 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:

175. The CCCC structure enables the capability to:

- reloutionize information exchange accross 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.

176. 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;
- Shared management information (status, availability);
- Global visibility;
- Interoperable resources;

A.15.2. CCCC Management Functions

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

178. **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.

179. **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.

180. **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.

181. 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

182. 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.

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

A.16. DEPLOYED CIS

184. The NISP 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 NISP has a part to play in resolving these issues.

185. 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 subnetting, 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.

A.17. DEPLOYED CIS

186. Linux (R) is the fastest growing operating system in the world. It already holds 34% of the Web market share. More and more developers, especially software companies, are focusing their efforts on creating Linux products. Even major corporations are currently responding. For instance, IBM, HP, Dell, Sun, and Oracle have all launched major initiatives, spending billions of dollars on Linux and Open Source software. It is anticipated that Linux and Linux based products, will provide a secure environment for defense oriented Web applications. Many defense organizations (e.g., the U.S. DoD) are moving toward Web-based architectures, even for combat operations. It is anticipated that the business decision to use freeware in conjunction with a simplified Web interface will save NATO, as well as NATO nations, billions of dollars. For military applications, the traffic needs to be encrypted and in dedicated networks using firewalls. However, such an environment will allow us to use this less expensive, dependable, and essentially common operating system. Linux DNS server, running BIND, can be configured to service Win95/98/2000/NT/XB clients. Linux also allows for the protection of data by using OpenSSH.

- Linux is Interoperable: Linux is compatible with the World Wide Web and can be configured to work with non-Linux clients and to network with non-Linux servers. Using this capability, NATO could set up multiple intranets which are Web-based to capitalize on potential interoperability concerns.

- Linux is Mature: Over one-third of the Web servers used today run Linux OS. Major vendors (see above) are investing billions of dollars in open source, Linux based, application solutions. LSB is based on POSIX (IEEE 1003.1-1990). Since the Open Group is currently developing test suites for LSB 1.1 and 1.2, it is anticipated that future versions of the LSB will fully conform to POSIX.1-2001.

- Linux is Implementable now: The fact that Linux is in used in over a third of the Web servers and used to develop real-time and embedded commercial products attests to the implement-ability of Linux.

- Linux is readily available: The LSB specifications are fee and publicly available at www.linuxbase.org.

This page is intentionally left blank

B. NISP RATIONALE DOCUMENT - TRACEABILITY MATRIX

B.1. INTRODUCTION

187. The NISP specifies the minimum set of communication and information technology standards to be mandated for the acquisition of all NATO C3 systems. In order to assist planners and developers of future C3 systems and major upgrades to existing C3 systems, it also contains a set of emerging standards. In order to be able to judge on the timeframe in which mandatory standards will phase out, or emerging will become mandatory, a standards Traceability Matrix has been developed. It tracks NOSWG decisions for including or deleting standards and also keeps history of why these decisions have been taken. The matrix is meant to provide a quick overview of all NISP standards and is considered complementary to the NISP Rationale Document. It is both a "forward looking" and "history" document, i.e. it guides acquisition and development of new and emerging information systems, and gives an indication what standards are fading out (thus providing a baseline towards which standards existing systems should move). It could also answer questions why certain standards have been selected, and while others have been disregarded. The purpose of the Traceability Matrix is to provide background on the NOSWG decisions on why NISP standards have been selected, deleted or are considered fading. It should be seen as an integral part of both the NISP as well as the Rationale Document.

188. The Traceability Matrix identifies each NISP service area, and presents all associated standards in tabular form in the same order as the NISP. The tables refine each service area into one or more functional classes, with each class mapping to one or more mandatory, emerging, or fading standards in a life-cycle history column. A Remarks column provides optional information on why this standard has been selected, deleted or is considered fading as of NISP version 3. For earlier versions of the NISP no tracking has taken place. Where a mandatory standard has been identified against a particular service class or sub-class, the implication is that the standard should be offered at the boundary interface. Where an emerging standard is identified, the expectation is that it is likely to become mandatory, but that for the time being it does not fulfil all of the criteria for mandation. Where a standard is considered fading, the belief is that the standard, although currently still supported by the market, will be overtaken by newer technology in the short term. Projects are to take this into account in their planning.

B.2. OPERATIONAL MISSION / ACTIVITIES / TASKS

B.3. USER INFORMATION SERVICES

B.4. TECHNICAL SERVICES

B.5. INFORMATION ASSURANCE

B.6. SERVICE MANAGEMENT AND CONTROL

This page is intentionally left blank