NATO STANDARD

ADatP-34

NATO Interoperability Standards and Profiles

Volume 1

Introduction

Edition N Version 2

5 May 2023

NORTH ATLANTIC TREATY ORGANIZATION
ALLIED DATA PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

The enclosed Allied Data Publication ADatP-34, Edition N, Version 2 NATO Interoperability Standards and Profiles, which has been approved by the nations in the C3B, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 5524.

ADatP-34, Edition N, Version 2 is effective on receipt.

This publication shall be handled in accordance with C-M(2002)60.

Dimitrios SIGOULAKIS
Major General, GRC (A)
Director, NATO Standardization Office

This page is intentionally left blank

RESERVED FOR NATIONAL LETTER OF PROMULGATION

This page is intentionally left blank

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

This page is intentionally left blank

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

This page is intentionally left blank

Table of Contents

CHAPTER 1. INTRODUCTION

001. The NATO Interoperability Standards and Profiles (NISP) is developed by the NATO Consultation, Command and Control (C3) Board Interoperability Profiles Capability Team (IP CaT).

002. The NISP will be made available to the general public as ADatP-34(N)(2) when approved by the C3 Board.

003. The included interoperability standards and profiles (Volume 2) are **mandatory** for use in NATO common funded Communications and Information Systems (CIS). Volume 3 contains **candidate** standards and profiles.

004. In case of conflict between any adopted non-NATO[1] standard and relevant NATO standard, the definition of the latter prevails.

005. In the NISP the keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [IETF RFC 2119].

Table 1.1. Abbreviations

Abbreviation	Full Text
ABB	Architecture Building Block
ACaT	Architecture Capability Team
ACP	Allied Communications Publication
AdatP-34	Allied Data Publication - Cover publication for the NISP
BSP	Basic Standards Profile
C3	Consultation, Command and Control
CCEB	Combined Communications Electronic Board (military communications-electronics organization established among five nations: Australia, Canada, New Zealand, United Kingdom, and the United States)
CESF	Core Enterprise Services Framework
COI	Community of Interest
CIAV (WG)	Coalition Interoperability Assurance and Validation (Working Group)

[1] ISO or other recognized non-NATO standards organization

Abbreviation	Full Text
CIS	Communication and Information Systems
CWIX	Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise
DOTMLPFI	Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability
EAPC	Euro-Atlantic Partnership Council
FMN	Federated Mission Networking
IOP	Interoperability Point
IP CaT	Interoperability Profiles Capability Team
MIP	Multilateral Interoperability Programme
NAF	NATO Architecture Framework
NDPP	NATO Defence Planning Process
NISP	NATO Interoperability Standards and Profiles
NIST	National Institute of Standards and Technology
NGO	Non govermental organization
RFC	Request for Change
SDS	Service Data Sheet
SIOP	Service Interoperability Point
SIP	Service Interface Profile
SME	Subject Matter Expert
SOA	Service Oriented Architecture
STANAG	A NATO standardization document that specifies the agreement of member nations to implement a standard, in whole or in part, with or without reservation, in order to meet an interoperability requirement. Notes: A NATO standardization agreement is distinct from the standard(s) it covers.
TACOMS	Tactical Communication Programme

1.1. PURPOSE OF THE NISP

006. NISP gives guidelines to capability planners, programme managers and test managers for NATO common funded systems in the short or mid-term timeframes.

007. The NISP prescribes the necessary technical standards and profiles to achieve interoperability of Communications and Information Systems in support of NATO's missions and operations. In accordance with the Alliance C3 Strategy (ref. C-M(2018)0037) all NATO Enterprise (ref. C-M(2014)0061) entities shall adhere to the NISP mandatory standards and profiles in volume 2.

1.2. INTENDED AUDIENCE

008. The intended audience of the NISP are all stakeholders in the NATO Enterprise, and Allied and Partner nations involved in development, implementation, lifecycle management, and transformation to a federated environment.

009. There are specific viewpoints that are mapped to the NISP structure. NISP gives guidelines to:

- capability planners involved in NDPP and NATO led initiatives
- programme managers for building NATO common funded systems
- test managers for their respective test events (such as CWIX, CIAV, etc.)
- national planning and programme managers for their national initiatives

010. Specific NATO or national views to the NISP based on data export to external planning and management systems will be possible upon delivery of an updated version of the NISP Exchange Specification.

This page is intentionally left blank

CHAPTER 2. BASIC CONCEPTS

011. This chapter gives an overview to understand the data in volume 2 and volume 3. NISP does not differentiate between the usage of NATO and non- NATO standards but always strives to select the most appropriate and up to date. The classification (Mandatory or Candidate) of any standard depends on its location in the NISP, Volume 2 or Volume 3, respectively.

2.1. STANDARDS

012. The NISP is composed of non-NATO and NATO Standards. While the first ones are adopted by NATO through the NISP. The second ones are to be considered as normative references.

013. Standards (NATO and non-NATO) are defined and managed in their life cycle by the developing standardization bodies with their own timetable. NATO standards are identified in the NISP by their covering document (STANAG number). They can be in the life cycle status of study/in ratification (no yet NATO approved/expected), promulgated (valid) and superseded/ obsolete. A non-NATO standard may have different life cycle status such as emerging, mature, fading, or obsolete. Different standardization bodies may use their own lifecycle status definitions. NISP takes lifecyle status of standards into account, but does not copy them into the NISP database. To inquire about the current status of NATO standards, please visit the NATO Standardization Document Database (NSDD) hosted on the NATO Standardization Organization (NSO) Website. Superseded/obsolete NATO and non-NATO standards may be included in the NISP for maintenance purpose.

014. NISP allow references to either a NATO Standard or the covering document if it exists. However, it is recommended that NATO organizations and nations reference a NATO Standard and NOT the covering document for inclusion in the NISP. IP CaT will subsequently add the covering document as well, but only for reference purposes.

2.2. INTEROPERABILITY PROFILES

015. Profiles define the specific use of standards at a service interoperability point (SIOP) in a given context. A SIOP is a reference point within an architecture where one or more service interfaces are physically or logically instantiated to allow systems delivering the same service using different protocols to interoperate. A SIOP serves as the focal point for service interoperability between interconnected systems, and may be logically located at any level within the components, and its detailed technical specification is contained within a service interface profile (SIP). Profiles support prerequisites for programmes or projects and enable interoperability implementation and testing.

016. Interoperability Profiles provide combinations of standards and (sub)profiles for different CIS and identify essential profile elements including:

- Capability Requirements and other NAF architectural views

- 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.

017. The NISP now defines the **obligation status** of profiles and standards as "mandatory" or "candidate".

- **Mandatory**: The application of standards or profiles is enforced for NATO common funded systems in planning, implementing and testing. Nations are required to use the NISP for developing capabilities that support NATO's missions (ie. NATO led operations, projects, programs, contracts and other related tasks). Nations are invited to do the same nationally to promote interoperabilty for federated systems and services.
- **Candidate**: The application of a standard or profile shall only be used for the purpose of testing and programme / project planning. The standard or profile must have progressed to a stage in its life-cycle and is sufficiently mature and is expected to be approved by the standardization body in the foreseeable future. This implies, that from a planning perspective, the respective standard or profile is expected to become mandatory during execution of the programme. A candidate standard or profile should not stay in volume 3 for more than 3 years.

018. Profiles shall be updated if referenced standards change. Profiles are dynamic entities by nature. NATO captures this dynamic situation by updating profiles once a year in the NISP. Profile owners are responsible for the versioning of their profiles. Profile reviews are required every 2 years by their owners to ensure their accuracy and continued relevance.

019. Proposed profiles (and standards) can be accepted as candidates in order to follow their developments and to decide if they can be promoted to mandatory standards and profiles. In some cases proposed standards and profiles can be readily accepted directly as mandatory.

020. Interoperability Profiles can reference other Interoperability Profiles to allow for maximal reuse.

021. Further information and guidance on creation of profiles is available in Appendix A.

2.3. BASIC STANDARDS PROFILE

022. Within the NISP, the "*Basic Standards Profile*" specifies the technical, operational, and business standards that are generally applicable in the context of the Alliance and the NATO Enterprise. For a specific context, such as Federated Mission Networking, separate profiles may

be defined that apply specifically to that context or related architectures. The standards that are cited may be NATO standards, or other agreed international and open standards.

023. As there is no overarching alliance architecture, each standard is associated with elements of the C3 Taxonomy. A distinction must be made between applicability of a standard, and conformance to the standard. If a standard is applicable to a given C3 Taxonomy element, any architecture that implements such an element need not be fully conformant with the standard. The degree of conformance may be judged based on the specific context of the project. For example, to facilitate information exchange between C2 and logistics systems it may be sufficient to implement only a subset of concepts as defined in JC3IEDM (STANAG 5525).

024. The “Basic Standards Profile” contains “agreed” as well as “candidate” standards.

2.4. CREATING RELATIONSHIPS TO OTHER CONCEPTS AND PLANNING OBJECTS WITHIN NATO

025. Different initiatives and organizations have developed new concepts to govern developments in the interoperability domain. These concepts have logical relationship to the NISP.

2.4.1. Architecture Building Block

026. An Architecture Building Block (ABB) is a constituent of the architecture model that describes a single aspect of the overall model [1].

2.4.1.1. Characteristics

027. ABBs:

- Capture architecture requirements; e.g., business, data, application, and technology requirements
- Direct and guide the development of Solution Building Blocks

2.4.1.2. Specification Content

028. ABB specifications include the following as a minimum:

- Fundamental functionality and attributes: semantic, unambiguous, including security capability and manageability
- Interfaces: chosen set, supplied
- Interoperability and relationship with other building blocks

[1] TOGAF 9.1 Specification

- Dependent building blocks with required functionality and named user interfaces
- Map to business/organizational entities and policies

2.4.2. FMN Spiral Specifications

029. Federated Mission Networking (FMN) Spiral[2] Specifications encompass "an evolutionary cycle that will raise the level of maturity of federated mission networking capabilities over time".

030. The FMN spiral specification contain the following sections

- architecture
- instructions
- profiles, and
- requirements specifications.

The Mandatory and Candidate FMN Spiral Profiles, in context for FMN Affiliates, are listed in the NISP Volumes 2 and 3.

2.4.3. Capability Packages

031. Profiles will be referenced in the NISP for specified NATO Common Funded Systems or Capability Packages and may include descriptions of interfaces to National Systems where appropriate.

2.5. CRITERIA FOR SELECTING STANDARDS

032. Any standard(s) listed in Volume 2 of the NISP shall:

- Be already approved by a NATO Standardization Tasking Authority or another non- NATO standards development organization (e.g. ISO, ANSI, ETSI, IEEE, IETF, W3C);
- Have an assigned responsible party within NATO that can provide relevant subject matter expertise;
- Be available in one of the NATO official languages;
- Support C3 Interoperability (including. people, processes and technology) and related NATO common funded Communication and Information Systems (CIS), including their development and operations;

[2]Annex B TO Volume I - Implementation Overview, NATO FMN Implementation Plan v4.0 dated: 23 September 2014, Terms and Definitions

- Enable the NATO Enterprise, NATO Nations and Partner Nations to develop interoperable C3 capabilities that support NATO's missions (i.e. NATO led operations, projects, programs, contracts and other related tasks).
- Any standard deviating from the criteria listed in this paragraph, can be recommended by the IP CaT for inclusion in the NISP and can be implemented after the approval of the C3B.

2.6. CRITERIA FOR SELECTING NON-NATO STANDARDS

033. Any Non-NATO standard(s) listed in Volume 2 of NISP should:

- Have implementations from a cross-section of vendors available;
- Be utilized by the broader user community;
- Be developed in a consensus-based way;
- Be free from any legal issues (i.e. intellectual property rights);
- Meet NATO requirements;
- Be easily accessible to vendors;
- Have an open architecture, e.g. extensible for new technological developments,
- Be compatible with other NATO-agreed standards;
- Be stable (mostly recognized by related community/industry) and mature enough in terms of technology;
- Be measurable in terms of its compliance.

This page is intentionally left blank

CHAPTER 3. ORGANIZATION OF THE NISP INFORMATION

034. This chapter gives an overview of the new structure of all three volumes.

3.1. NISP STRUCTURE

035. The structure of the NISP is organized to list and categorize the standards and profiles according to their usage in NATO. It contains three volumes:

- **Volume 1** - Introduction: This volume introduces basic concepts, provides the management framework for the configuration control of the NISP and the process for handling Request for Change (RFC). It includes also guidance on development of interoperability profiles.
- **Volume 2** - Agreed Interoperability Standards and Profiles: This volume lists agreed interoperability standards and profiles, mandatory for NATO common funded systems. These should support NATO and National systems today and new systems actually under procurement or specification.
- **Volume 3** - Candidate Interoperability Standards and Profiles: This Volume lists informative references to Standards and Interoperability Profiles, such as drafts of NATO specifications, that may be used as guidance for future programmes.

036. Volume 2 is normative for NATO common funded systems and Volume 3 is informative.

This page is intentionally left blank

CHAPTER 4. INTEROPERABILITY IN SUPPORT OF CAPABILITY PLANNING

037. The following documents form the foundation to understand the embedding of NISP into NDPP and architecture work:

Table 4.1. NDPP References

Document	Document Reference
Alliance C3 Strategy Information and Communication Technology to prepare NATO 2020 (20 July 2018)	Alliance C3 Strategy C-M(2018)0037
Alliance C3 Policy (14 December 2018)	C-M(2015)0041-REV2
NATO Defence Planning Process (NDPP)	PO(2016)0655 (INV)

038. The NATO Defence Planning Process (NDPP) is the primary means to identify the required capabilities and promote their timely and coherent development and acquisition by Allies and Partners. It is operationally driven and delivers various products which could support the development and evolution of more detailed C3 architecture and interoperability requirements. The development of NDPP products also benefits from input by the architecture and interoperability communities, especially the NISP, leading to a more coherent development of CIS capabilities for the Alliance.

039. The work on Enterprise, Capability, and programme level architecture will benefit from the NISP by selecting coherent sets of standards for profiles.

040. More information on how the NISP supports the NDPP can be found in Annex B.

This page is intentionally left blank

CHAPTER 5. CONFIGURATION MANAGEMENT

041. The NISP is updated once a year to account for the evolution of standards and profiles.

042. Request for Change (RFC) to the NISP will be processed by the IP CaT, following the process in the graphic below:

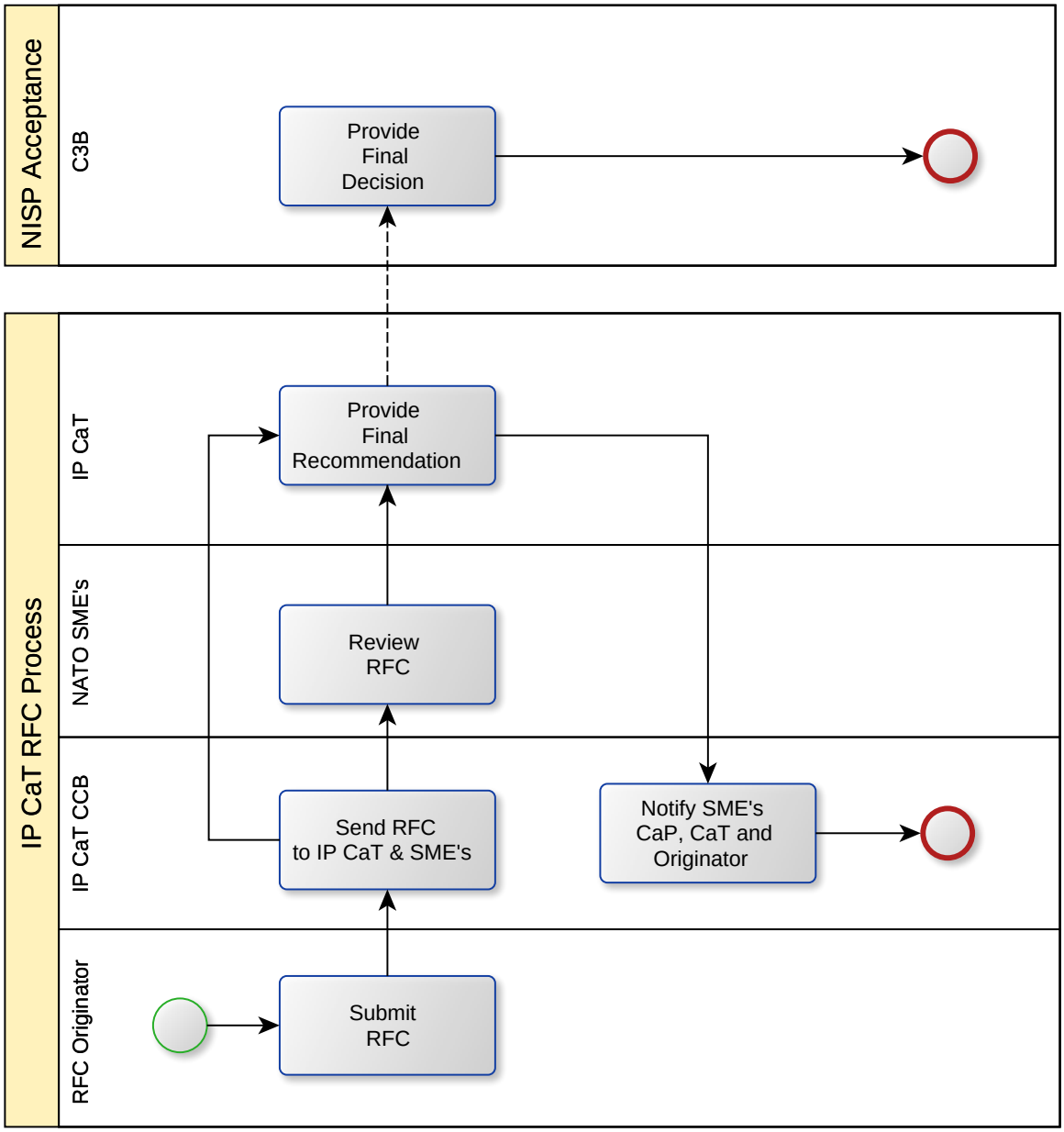

Figure 5.1. RFC Handling Process

043. The RFC contains all information required for the NISP management by IP CaT; The detailed information about standard or profile is handed over as attachments to this form. A notional RFC form with example information is presented below:

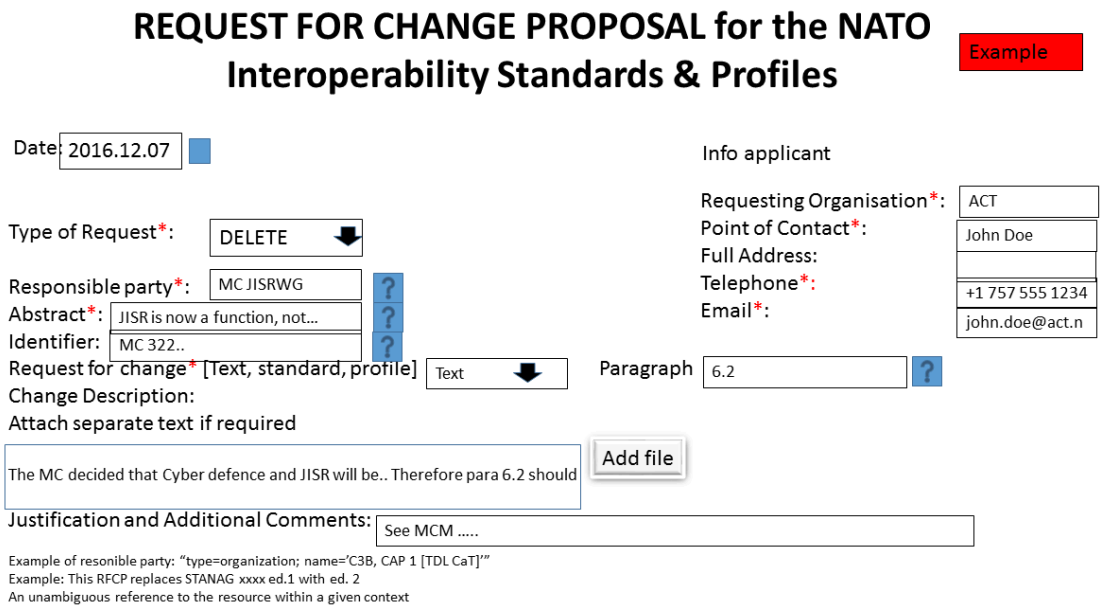

Figure 5.2. RFC Notional Form

044. The primary point of contact for RFC submission is the IP CaT. RFCs may be submitted to the IP CaT via the Change web site or via email to herve.radiguet@act.nato.int with attachments.

045. Review of RFCs will be coordinated with the responsible C3 Board substructure organizations where appropriate.

046. The IP CaT reviews the submissions in dialog with national and international bodies. Based on that review, the RFC will be formally processed into the next version of the NISP; or returned to the originator for further details; or rejected. The IP CaT will attempt to address all RFCs submitted by 1 September into the next NISP release. RFCs submitted after this date may be considered for inclusion at the discretion of the IP CaT, or will be processed for the following NISP release.

5.1. NISP UPDATE PROCESS

047. The new NISP version is submitted to the C3 Board by end of the year after internal review by the IP CaT. The version under review is a snapshot in time of the status of standards and profiles.

048. The database of standards and profiles maintained by the IP CaT is the definitive source of the current status of standards and profiles.

5.1.1. Criteria for listing Standards and Profiles

049. Standards and profiles listed in Volume 2 of the NISP shall:

1. have an assigned responsible party that can provide relevant subject matter expertise, if no responsible party exists the IP CaT will create a temporary assignment,

2. be available in one of the NATO official languages,

3. support C3 Interoperability (incl. people, processes and technology) and related NATO common funded Communication and Information Systems (CIS) including their development and operations, and

4. enable the NATO Enterprise, NATO Nations and partner nations to develop interoperable capabilities that support NATO's missions (ie. NATO led operations, projects, programs, contracts and other related tasks).

050. In addition standards shall be approved already by a NATO Standardization Tasking Authority or another non-NATO standards development organization (e.g. ISO, ANSI, ETSI, IEEE, IETF, W3C).

051. Deviations from the rules listed above can be recommended by the IP CaT and approved by the C3B.

052. Given the rate of innovation in Information and Communication Technology (ICT), it is unsurprising that, NATO standards must be reviewed and updated regularly to keep pace with the state of the art and other international standards. The following criteria should be considered by responsible parties during their annual review of NATO Standards:

- Are all stakeholders' views are reflected in the Standardization Working Group?
    - End Users/ Operational Users
    - Implementers/Vendors
    - Technical Solutions Experts/Testers
    - Standards Experts
- Are all referenced basic standards and documents still valid?
- Are key terms consistent with agreed NATO Terminology?
- Does the standard contain conformance criteria?
- Were any issues with the standard identified during test events (e.g. CWIX, CIAV)?

- Are reference implementations[1] of the Standard available to vendors?

053. Some key criteria for inclusion of non-NATO standards into Volume 2 are

- Availability of implementations from a cross-section of vendors;
- Compatibility with other standards;
- Completeness. Does the standard meet the functional requirements?
- Extensibility. Can the standard easily add new technologies when they become available?;
- Stability/maturity. Is the standard based on well understood technology, and has it matured enough to ensure no major changes will occur through further refinements?
- Non-discriminatory. Was the standard developed in a consensus-based way?
- Testability. Conformance metrics. Can the standard be tested to prove compliance?
- Legitimacy. Freedom from legal issues.

054. Similar criteria are also applied for inclusion of Profiles into Volume 2. Profiles should follow the Profile Guidance in Volume 1, Appendix A, and the IPCaT reserves the right to adjust the data structure of a profile to align with the data model of the NISP.

055. Standards and profiles listed in Volume 3 are not subject to the above criteria as they are not (yet) mandatory.

5.1.2. Updating listed Standards and Profiles

- process RFCs together with related responsible parties,
- check if newer versions of
  - listed standards are published by the NATO Standardization Tasking Authority or another non-NATO standards development organization,
  - listed profiles are published by the respective development organization,
  - contact all responsible parties to assess if there is a continued need to keep standards and profiles within Volume 2.

[1]To facilitate interoperability and adoption in general the production of reference implementations and similar tools that vendors can use to bootstrap and test development efforts is critical. These reference tools help clarify the expected behavior described by the standard. If these tools are released under appropriate licenses, the tools themselves or components thereof can be directly integrated into vendor products, reducing the investment cost, and therefore the risk, of adoption and accelerating adoption efforts. For standards that rely on multiple parties, such as communications protocols between two different roles, having a reference implementation for both communicants can be a big help to implementers by giving them a correspondent against which to test their own implementation. As such, simple implementation efforts can have a significant role in encouraging interoperability and adoption.

5.2. NISP PRODUCTS

056. The NISP is published in several formats:

- Documentation in HTML and PDF Formats
- Website and searchable online Database
- Data export in ArchiMate Exchange File Format

This page is intentionally left blank

CHAPTER 6. NATIONAL SYSTEMS INTEROPERABILITY COORDINATION

057. Coordination of standards and profiles between Nations and NATO are critical for interoperability. As a result of the C3 Board substructure reorganization, participants in IP CaT are subject matter experts (SME) and are no longer national representatives. SME's should therefore coordinate with national and C3 Board representatives to ensure national perspectives are presented to IP CaT. As such, each of the IP CaT SMEs is responsible for:

- Appropriate and timely coordination of standards and profiles with respect to interoperability with national systems;
- Coordination of the SME input including coordination with national SMEs of other C3 Board substructure groups; and
- Providing appropriate technical information and insight based on national market assessment.

058. National level coordination of interoperability technical standards and profiles is the responsibility of the C3 Board. When the latest version of NISP is approved by the C3 Board, it will become the NATO Standard covered by STANAG 5524. This STANAG contains the agreement of the participating nations regarding usage of the mandatory standards and profiles in the NISP.

This page is intentionally left blank

CHAPTER 7. INTEROPERABILITY STANDARDS GUIDANCE

059. The NISP references Standards from different standardization bodies[1]. In the case of a ratified STANAG, NATO standardization procedures apply. The NISP only references these STANAG's without displaying the country-specific reservations. The country-specific reservations can be found in the NATO Standardization Office's NATO Standardization Document Database.

060. The Combined Communications Electronics Board (CCEB) nations will use NISP Volume 2 to publish the interoperability standards for the CCEB under the provisions of the NATO-CCEB List of Understandings (LoU)[2].

061. The NISP organizes the standards using the structure of baseline 5.0 of NATO's C3 Taxonomy, as endorsed by the NATO C3 Board per AC/322-D(2021)0021 on "C3 Taxonomy Baseline 5.0" dated 23 September 2021. A graphical representation of this taxonomy is given in the following figure and a description of it can be obtained at: https://tide.act.nato.int/mediawiki/tidepedia/index.php/C3_Taxonomy_Baseline_5. Currently, the standards only address a subset of the services in the taxonomy, mainly services in the group Technical Services. For some standards it is indicated that an appropriate mapping to the C3 Taxonomy could not yet be made.

[1]In case of conflict between any adopted non-NATO standard and relevant NATO standard, the definition of the latter prevails.
[2]References: NATO Letter AC/322(SC/5)L/144 of 18 October 2000, CCEB Letter D/CCEB/WS/1/16 of 9 November 2000, NATO Letter AC/322(SC/5)L/157 of 13 February 2001

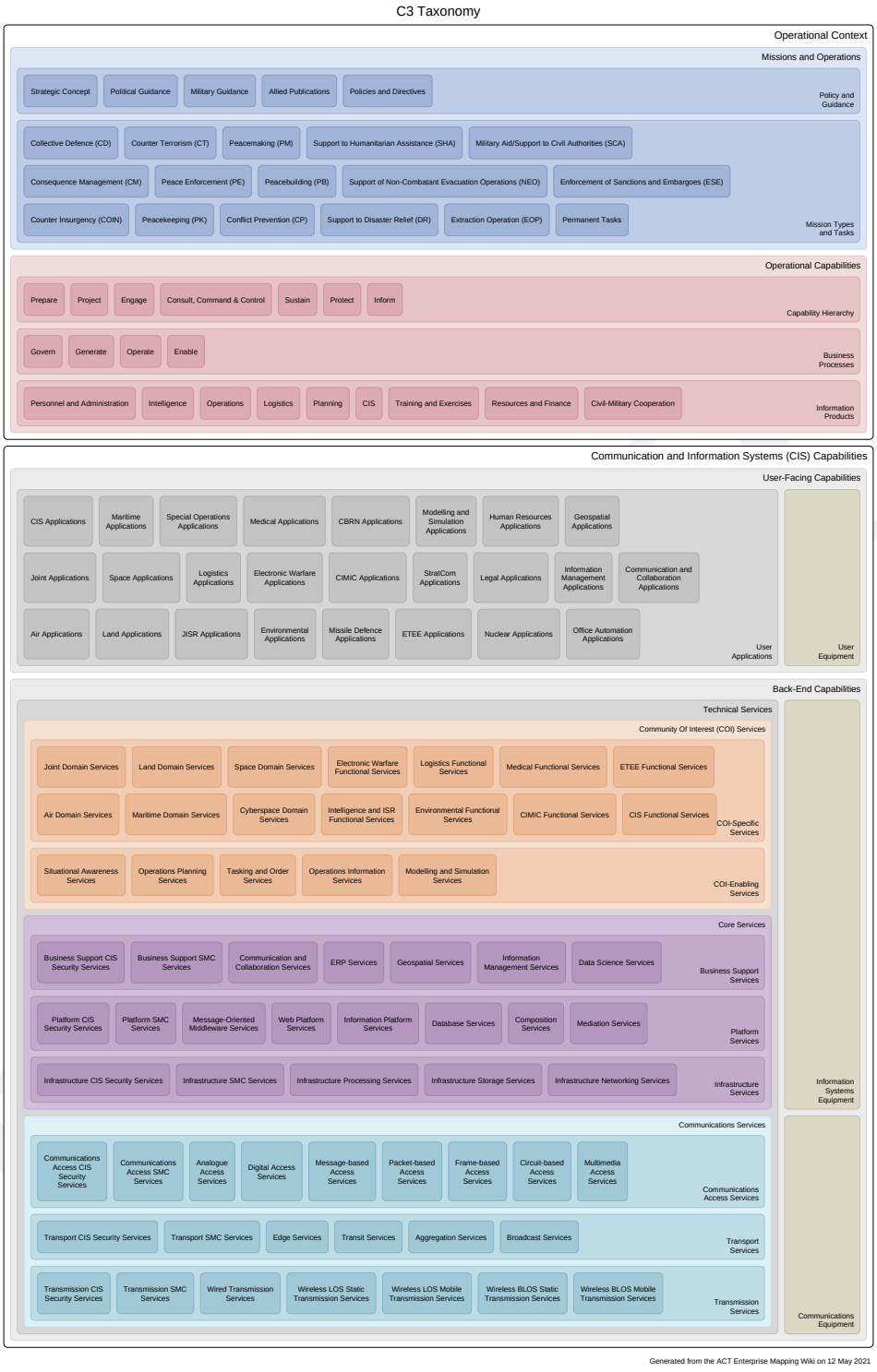

Figure 7.1. C3 Taxonomy

062. In principle, NISP only contains or references standards or related documents, which are generally available for NATO/NATO member nations/CCEB.

063. However, a subset of documents may only be available for those nations or organizations, which are joining a specific mission or are members of a special working group. The membership in these activities is outside the scope of NISP.

This page is intentionally left blank

CHAPTER 8. APPLICABILITY

064. The mandatory standards and profiles documented in Volume 2 will be used in the implementation of NATO Common Funded Systems. Participating nations agree to use the mandatory standards and profiles included in the NISP at the Service Interoperability Points and to use Service Interface Profiles among NATO and Nations to support the exchange of information and the use of information services in the NATO realm.

This page is intentionally left blank

APPENDIX A. PROFILE GUIDANCE

A.1. PROFILE CONCEPTUAL BACKGROUND

065. ISO/IEC TR 10000 [2] 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.

066. The C3 Board (C3B) Interoperability Profiles Capability Team (IP CaT) has extended the profile concept to encompass references to NAF architectural views [1], characteristic protocols, implementation options, technical standards, Service Interoperability Points (SIOP), and related profiles.

067. Nothing in this guidance precludes the referencing of National profiles or profiles developed by non-NATO organizations in the NATO Interoperability Standards and Profiles (NISP).

A.2. PURPOSE OF INTEROPERABILITY PROFILES

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

069. Interoperability Profiles identify essential profile elements including Capability Requirements and other NAF architectural views [1], 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.

070. NATO and Nations use profiles to ensure that all organizations will architect, invest, and implement capabilities in a coordinated way that will 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.

A.3. APPLICABILITY

071. NISP stakeholders include engineers, designers, technical project managers, procurement staff, architects and other planners. Architectures, which identify the components of system operation, are most applicable during the development and test and evaluation phase of a project. The NISP is particularly applicable to a federated environment, where interoperability of mature National systems requires an agile approach to architectures.

072. The IP CaT 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.

A.4. GUIDELINES FOR INTEROPERABILITY PROFILE DEVELOPMENT

073. 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
- Develop modular Architecture Building Blocks
- Use standards consistent with common architectures
- Develop specifications that are service oriented and independent of the technology implemented in National systems where practical
- Develop modular profiles that are reusable in future missions or capability areas
- Use an open system approach to embrace emerging technologies

074. 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.

075. The NISP is the governing authoritative reference for NATO interoperability profiles. Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and Interoperability (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.

A.5. STRUCTURE OF INTEROPERABILITY PROFILE DOCUMENTATION

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

A.5.1. Identification

077. 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.

A.5.2. Profile Elements

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

079. 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 applications 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'.

A.5.2.1. Applicable Standards

080. Each profile **should** 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 A.1. Applicable Standards

ID	Purpose/Service	Standards	Guidance
A unique profile identifier	A description of the purpose or service	A set of relevant Standard Identifier from the NISP	Implementation specific guidance associated with this profile (may be a reference to a separate annex or document)

A.5.2.2. Related Profiles

081. 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 A.2. 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

A.6. VERIFICATION AND CONFORMANCE

082. Each profile **should** 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. All performance requirements must be quantifiable and measurable; each requirement must include a performance (what), a metric (how measured), and a criterion (minimum acceptable value).

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

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

1. Approach to Validating Service Interoperability Points
2. Relevant Maturity Level Criteria
3. Key Performance Indicators (KPIs)
4. Experimentation
5. Demonstration

A.6.1. Approach to Validating Service Interoperability Points

085. 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).

A.6.2. Relevant Maturity Level Criteria

086. Each profile should describe the Maturity criteria applicable to the profile. The intention of this section is to describe how this profile supports the achievement of improved interoperability.

A.6.3. Key Performance Indicators (KPIs)

087. 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 A.3. Key Performance Indicators (KPIs)[1]

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	

[1]'notional' KPIs shown in the table are for illustrative purposes only.

A.6.4. Experimentation

088. 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.

A.6.5. Demonstration

089. 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.

A.7. CONFIGURATION MANAGEMENT AND GOVERNANCE

A.7.1. Configuration Management

090. 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 IP CaT].

A.7.2. Governance

091. Each profile **shall** identify **one or more authorities** to provide feedback and when necessary, Request for Change (RFC) 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.

References

[1] *NATO Architecture Framework Version 4*. 25 January 2018. AC/322-D(2018)0002.

[2] *Information Technology - Framework and Taxonomy of International Standardized Profiles - Part 3: Principals and Taxonomy for Open System Environment Profiles*. Copyright # 1998. ISO. ISO/IEC TR 10000-3.

APPENDIX B. INTEROPERABILITY IN THE CONTEXT OF NATO DEFENCE PLANNING

B.1. NATO DEFENCE PLANNING

092. The NATO Defence Planning Process (NDPP) is the primary means to identify required capabilities and promote their timely, coherent development and acquisition by Allies and the NATO Enterprise. It is operationally driven and delivers various products which could support the development and evolution of more detailed C3 architecture and interoperability requirements. The development of NDPP products also benefits from input by the architecture and interoperability communities, especially the NISP, leading to a more coherent development of CIS capabilities for the Alliance.

093. Ideally technical interoperability requirements align with the NDPP to ensure coherence in the development of capabilities within the Alliance. NDPP Mission Types and Planning Situations provide the essential foundation for the development of the Minimum Capability Requirements (MCR) and the derivation of high level information exchange and interoperability requirements. MCRs are expressed via a common set of definitions for capabilities (including CIS) called Capability Codes and Statements (CC&S), including explicit reference to STANAGs in some cases[1]. Interoperability aspects are primarily captured in free text form within the Capability Statements and in the subsequent NDPP Targets[2]. The NDPP products could be leveraged by the architecture and interoperability community, to define the operational context for required Architecture Building Blocks and interoperability profiles.

094. The Defence Planning Capability Survey (DPCS) is the tool to collect information on national capabilities, the architecture and interoperability communities should provide input on questions related to C3 related capabilities. The architecture and interoperability communities could also bring valuable insight and expertise to the formulation and tailoring of C3 capabilities-related targets to nations, groups of nations or the NATO enterprise.

095. In practice, there is not always an opportunity (time or money) for such a "clean" approach and compromises must be made - from requirements identification to implementation. In recognition of this fact, NATO has developed a parallel track approach, which allows some degree of freedom in the systems development. Although variations in sequence and speed of the different steps are possible, some elements need to be present. Architecture, including the selection of appropriate standards and technologies, is a mandatory step.

096. In a top-down execution of the systems development approach, architecture will provide guidance and overview to the required functionality and the solution patterns, based on longstanding and visionary operational requirements. In a bottom-up execution of the approach, which may be required when addressing urgent requirements and operational imperatives,

[1]Bi-SC Agreed Capability Codes and Capability Statements, 29 July 2016 and SH/SDP/SDF/CFR/DPF/20-006166 and ACT/SPP/DP/TT-2897/Ser:NU0074 issued on 29 July 2020.
[2]C-M(2017)0021, NATO Capability Targets, 26 June 2017

architecture will be used to assess and validate chosen solution in order to align with the longer term vision.

097. The NISP is a major tool supporting NATO architecture work and must be suitable for use in the different variations of the systems development approach. The NISP will be aligned with the Architectural efforts of the C3 Board led by the ACaT.

098. The relationship of the NISP, the Architecture Building Blocks activities of the ACaT, and Allied Command Transformation Architecture efforts is of a mutual and reciprocal nature. Architecture products provide inputs to the NISP by identifying the technology areas that in the future will require standards. These architecture products also provide guidance on the coherence of standards by indicating in which timeframe certain standards and profiles are required. NATO Architectures benefit from the NISP by selecting coherent sets of standards from profiles.

APPENDIX C. CHANGES

099. Major content changes Changes from NISP Version 14 / ADatP-34(N)(1) to NISP Version 15 / ADatP-34(N)(2) include:

- Draft FMN Spiral 5 Profile added as candidate (Vol 3).
- 55 RFCs processed. Details of the RFC changes are captured in Appendix E.
- Removed C3 Taxonomy v4
- Added C3 Taxonomy v5
- Major cleanup of the NISP database

This page is intentionally left blank

APPENDIX D. DETAILED CHANGES

100. Detailed content Changes from NISP Version 14 / ADatP-34(N)(1) to NISP Version 15 / ADatP-34(N)(2) includes:

D.1. Added Standards

D.1.1. ASCA

- Common Technical Interface Design Plan (CTIDP) (ASCA ASCA-012:2021)

D.1.2. CCEB

- Communications Instructions Tape Relay Procedures (CCEB ACP 127(G):1988)

D.1.3. CIS3 C&IP

- SCIP Signalling Plan rev.3.10 (CIS3 C&IP SCIP-210 3.10:2017)

D.1.4. DIGWG

- Defence Profile of OGC Web Coverage Service 2.0 (DIGWG DGIWG-119:2017)
- Defence Profile of OGC Web Feature Service 2.0 (DIGWG DGIWG-122:2019)
- Defense Gridded Elevation Data (DGED) Product Implementation Profile (DIGWG DGIWG-250:2020)

D.1.5. IETF

- JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens (IETF RFC 9068:2021)

D.1.6. ISO/IEC

- Computer graphics and image processing — Portable Network Graphics (PNG): Functional specification (ISO/IEC 15948:2004)
- Generic coding of moving pictures and associated audio information — Part 7: Advanced Audio Coding (AAC) — Amendment 1: Transport of MPEG Surround in AAC (ISO/IEC 13818-7:2006/Amd 1:2007)
- Generic coding of moving pictures and associated audio information — Part 7: Advanced Audio Coding (AAC) — Technical Corrigendum 1 (ISO/IEC 3818-7:2006/Cor 1:2009)
- Generic coding of moving pictures and associated audio information — Part 7: Advanced Audio Coding (AAC) — Technical Corrigendum 2 (ISO/IEC 3818-7:2006/Cor 2:2010)
- Coding of audio-visual objects — Part 10: Advanced video coding (ISO/IEC 14496-10:2022)

D.1.7. MIP

- MIP Information Model 5.1 (MIP MIM 5.1:2020)

D.1.8. NATO

- VLF / LF MSK Multi Channel Broadcast (NATO AComP-4724 Ed B Ver 1:2021)
- Concept of NATO Message Text Formatting System (CONFORMETS) (NATO ADatP-03 Ed A Ver 4:2006)
- Tactical Data Exchange - Link 1 (Point-to-Point) (NATO ATDLP-5.01 Ed A Ver 2:2020)
- Land Operational Reports (NATO ATP-105 Ed A Ver 1:2021)
- NATO Land Urgent Voice Messages (LUVM) Pocket Book (NATO ATP-97 Ed B Ver 1:2020)
- Joint C3 Information Exchange Data Model Baseline 3.1.4 (NATO JC3IEDM Baseline 3.1.4:2012)
- Allied Joint Doctrine for Maritime Operations - AJP-3.1 EDITION A (NATO STANAG 1459 ED 3:2016)
- LAND OPERATIONAL REPORTS (NATO STANAG 2020 Ed 4:2021)
- NATO Land Urgent Voice Messages (LUVM) Pocket Book - ATP-97 Edition B (NATO STANAG 2627 Ed 2:2020)
- VLF / LF MSK Multi Channel Broadcast - AComP-4724 Edition A (NATO STANAG 4724 Ed 2:2021)
- Networking and Information Infrastructure (NII) Internet Protocol (IP) Network Encryptor – Interoperability Specification (NINE ISPEC) - AComP-4787 Edition A (NATO STANAG 4787 Ed 1:2018)
- Joint Range Extension Application Protocol (JREAP) - ATDLP-5.18 Edition B Version 2 (NATO STANAG FT 5518 Ed 5)
- Standards for Data Forwarding between Tactical Data Systems (NATO STANAG 5616 Ed 8:2021)
- Narrowband Waveform for VHF/UHF Radios - AComP-5630-5633 Edition A (NATO STANAG 5630 Ed 1:2019)
- NATO IFF MK XIIA and MODE S Test Guidance and Tests Requirements Documentation Package (NATO STANAG 5647 Ed 1:2019)
- NATO High Capacity Data Rate Waveform (NHCDRWF) - AComP-5649 Edition A (NATO STANAG (Study) 5649 Ed 1)
- NATO High Data Rate Waveform (NHDRWF) - AComP-5651 (Study) EDITION A (NATO STANAG (Study) 5651 Ed 1)
- NATO Core Data Framework (NCDF) - ADatP-5653 Edition A (NATO STANAG (Study) 5653 Ed 1)
- GeoTIFF Raster Format Specification in a NATO Environment (NATO AGeoP-11.3 Ed A Ver 1:2018)
- SATURN - A Fast Frequency Hopping ECCM Mode for UHF Radio (NATO STANAG 4372 Ed 4:2019)
- SATURN - A Fast Frequency Hopping ECCM Mode for UHF Radio (NATO AComP-4372 Ed A Ver 1:2019)
- Interoperability between Ultra High Frequency Satellite Communications (UHF SATCOM) Terminals - Integrated Waveform (IW) (NATO STANAG 4681 Ed 2:2022)

- Interoperability between Ultra High Frequency Satellite Communications (UHF SATCOM) Terminals - Integrated Waveform (IW) (NATO AComP-4681 Ed A Ver 1:2022)
- Allied Maritime Tactical Instructions and Procedures (NATO STANAG 1173 Ed 26:2021)
- Allied Maritime Tactical Instructions and Procedures (NATO MTP-01 Ed H:2021)
- NATO Message Text Formatting System (FORMETS) - ADatP-3 (NATO STANAG 5500 Ed 4:1966)
- NATO Message Text Formatting System (FORMETS) (NATO ADatP-03 Baseline-11 (Current):1999)
- NATO Message Text Formatting System (FORMETS) (NATO ADatP-03 Baseline-11 (Future):1999)

D.1.9. NATO Study (expected)

- Joint Range Extension Application Protocol (JREAP) (NATO Study (expected) ATDLP-5.18 (Study) Ed C Ver 1)
- Tactical Data Exchange - Link 16 (NATO Study (expected) ATDLP-5.16 Ed C Ver 1:2019)
- Tactical Data Exchange - Link 16 - ATDLP-5.16 Edition C Version 1 (NATO Study (expected) STANAG FT (Study) 5516 Ed 9)

D.1.10. NIST

- Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (NIST SP 800-56A Rev 2:2013)

D.1.11. OGC

- Web Services Common Implementation Specification v1.1.0 with Corrigium 1 (OGC 06-121r3:2007)
- Corrigendum for OpenGIS Implementation Standard Web Processing Service (WPS) 1.0.0 (OGC 08-091r6:2009)
- GML in JPEG 2000 for Geographic Imagery Encoding (OGC 08-085r8:2018)

D.1.12. TM-FORUM

- Service Catalog API User Guide (TM-FORUM TMF633 (2021/01):2021)

D.1.13. US DoN

- Operational Specification for Over-The-Horizon Targeting Gold Revision D, OS-OTG (Rev. D) (US DoN OTH-T Gold Baseline 2000:2000)

D.1.14. XMPP

- XEP-0297: Stanza Forwarding (XMPP XEP-0297:2013)

D.2. Deleted standards

D.2.1. C3B

- NII Communications Reference Architecture Edition 1, Version 1.2 (C3B AC/322-D(2010)0035:2010)

D.2.2. DMTF

- CIM Schema: Version 2.30.0 (DMTF CIM V2300:2011)
- Common Information Model (CIM) v2.2 (DMTF DSP0004:1999)
- Web Services for Management (WS-Management) Specification (DMTF DSP0226:2010)
- WS-Management CIM Binding Specification (DMTF DSP0227:2010)
- Configuration Management Database (CMDB) Federation Specification (DMTF DSP0252:2010)

D.2.3. IEEE

- Distributed Interactive Simulation (DIS) - Exercise Management and Feedback (IEEE P1278.3:1996)

D.2.4. IETF

- Open Network Computing (ONC) Remote Procedure Call (RPC) Specification version 2 (IETF RFC 1057:1988)
- PPP LCP Extensions (IETF RFC 1570:1994)
- Extensions to OSPF to support demand circuits (IETF RFC 1793:1995)
- The LDAP Application Program Interface (IETF RFC 1823:1995)
- An Aplication of the BGP Community Attribute in Multi-Home Routing (IETF RFC 1998:1996)
- IP Encapsulation within IP (IETF RFC 2003:1996)
- Portable Network Graphics (PNG) Specification, v. 1.0 (IETF RFC 2083:1997)
- ISO Transport Service on top of TCP (ITOT) (IETF RFC 2126:1997)
- Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification (IETF RFC 2205:1997)
- RSVP Management Information Base using SMIv2 (IETF RFC 2206:1997)
- RSVP Extensions for IPSEC Data Flows (IETF RFC 2207:1997)
- Resource ReSerVation Protocol (RSVP) -- Version 1 Applicability Statement Some Guidelines on Deployment (IETF RFC 2208:1997)
- Resource ReSerVation Protocol (RSVP) -- Version 1 Message Processing Rules (IETF RFC 2209:1997)
- The Use of RSVP with IETF Integrated Services (IETF RFC 2210:1997)
- FTP Security Extensions (IETF RFC 2228:1997)
- Using LDAP as a Network Information Service (IETF RFC 2307:1998)

- IPv6 Multicast Address Assigments (IETF RFC 2375:1998)
- FTP Extensions for IPv6 and NATs (IETF RFC 2428:1998)
- A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE) (IETF RFC 2430:1998)
- Transmission of IPv6 Packets over Ethernet Networks (IETF RFC 2464:1998)
- Transmission of IPv6 Packets over FDDI Networks (IETF RFC 2467:1998)
- Generic Packet Tunneling in IPv6 (IETF RFC 2473:1998)
- A Simulation Model for IP Multicast with RSVP (IETF RFC 2490:1999)
- IPv6 over Non-Broadcast Multiple Access (NBMA) networks (IETF RFC 2491:1999)
- IP Header Compression (IETF RFC 2507:1999)
- Compressing IP/UDP/RTP Headers for Low-Speed Serial Links (IETF RFC 2508:1999)
- Lightweight Directory Access Protocol (LDAP) v3 - Extensions for Dynamic Directory Services (IETF RFC 2589:1999)
- Internationalization of the File Transfer Protocol (IETF RFC 2640:1999)
- An LDAP Control and Schema for Holding Operation Signatures (IETF RFC 2649:1999)
- LDAP Control Extension for Simple Paged Results Manipulation (IETF RFC 2696:1999)
- Multicast Listener Discovery (MLD) for IPv6 (IETF RFC 2710:1999)
- IPv6 Router Alert Option (IETF RFC 2711:1999)
- RSVP Diagnostic Messages (IETF RFC 2745:2000)
- RSVP Operation Over IP Tunnels (IETF RFC 2746:2000)
- RSVP Cryptographic Authentication (IETF RFC 2747:2000)
- COPS usage for RSVP (IETF RFC 2749:2000)
- RSVP Extensions for Policy Control (IETF RFC 2750:2000)
- A Framework for Policy-based Admission Control (IETF RFC 2753:2000)
- Encryption using KEA and SKIPJACK (IETF RFC 2773:2000)
- SBM (Subnet Bandwidth Manager): A Protocol for RSVP-based Admission Control over IEEE 802-style networks (IETF RFC 2814:2000)
- LDAP Control Extension for Server Side Sorting of Search Results (IETF RFC 2891:2000)
- Router Renumbering for IPv6 (IETF RFC 2894:2000)
- RSVP Refresh Overhead Reduction Extensions (IETF RFC 2961:2001)
- Format of the RSVP DCLASS Object (IETF RFC 2996:2000)
- Framework for Integrated Services Operation over Diffserv Networks (IETF RFC 2998:2000)
- Traditional IP Network Address Translation (NAT) (IETF RFC 3022:2001)
- Multiprotocol Label Switching Architecture (IETF RFC 3031:2001)
- MPLS Label Stack Encoding (IETF RFC 3032:2001)
- Storing Vendor Information in the LDAP root DSE (IETF RFC 3045:2001)
- Connection of IPv6 Domains via IPv4 Clouds (IETF RFC 3056:2001)
- LDAP Password Modify Extended Operation (IETF RFC 3062:2001)
- Differentiated Services Per Domain Behaviours and Rules for their Specification (IETF RFC 3086:2001)
- Service Location Protocol Modifications for IPv6 (IETF RFC 3111:2001)
- Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification (IETF RFC 3122:2001)

- Transmission of IPv6 Packets over IEEE 1394 Networks (IETF RFC 3146:2001)
- RADIUS and IPv6 (IETF RFC 3162:2001)
- Aggregation of RSVP for IPv4 and IPv6 Reservations (IETF RFC 3175:2001)
- Signalled Preemption Priority Policy Element (IETF RFC 3181:2001)
- Identity Representation for RSVP (IETF RFC 3182:2001)
- RSVP-TE: Extensions to RSVP for LSP Tunnels (IETF RFC 3209:2001)
- Applicability Statement for Extensions to RSVP for LSP-Tunnels (IETF RFC 3210:2001)
- IANA Assigned Numbers (IETF RFC 3232:2002)
- Stream Control Transmission Protocol Applicability Statement (IETF RFC 3257:2002)
- New Terminology and Clarifications for Diffserv (IETF RFC 3260:2002)
- Stream Control Transmission Protocol - Introduction (IETF RFC 3286:2002)
- Remote Monitoring MIB Extensions for Differentiated Services (IETF RFC 3287:2002)
- Management Information Base for the Differentiated Services Architecture (IETF RFC 3289:2002)
- Informal Management Model for Diffserv Routers (IETF RFC 3290:2002)
- Named Subordinate References in LDAP Directories (IETF RFC 3296:2002)
- Unicast-Prefix-based IPv6 Multicast Addresses (IETF RFC 3306:2002)
- Allocation Guidelines for IPv6 Multicast Addresses (IETF RFC 3307:2002)
- Layer Two Tunnelling Protocol (L2TP) Differentiated Services Extension (IETF RFC 3308:2002)
- Transport Layer Security over Stream Control Transmission Protocol (IETF RFC 3436:2002)
- The Multiprotocol Label Switching (MPLS) Working Group decision on MPLS signalling protocols (IETF RFC 3468:2003)
- Generalized Multi-Protocol Label Switching (GMPLS) Signalling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions (IETF RFC 3473:2003)
- IANA assignments for GMPLS and RSVP-TE Extensions for ASON (IETF RFC 3474:2003)
- IANA assignments for LDP, RSVP, and RSVP-TE Extensions for Optical UNI Signaling (IETF RFC 3476:2003)
- Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE) (IETF RFC 3477:2003)
- A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block (IETF RFC 3531:2003)
- IP Header Compression over PPP (IETF RFC 3544:2003)
- On the Use of Stream Control Transmission Protocol (SCTP) with IPsec (IETF RFC 3554:2003)
- Ad-hoc On-Demand Distance Vector Routing (AODV) (IETF RFC 3561:2003)
- Textual Conventions for IPv6 Flow Label (IETF RFC 3595:2003)
- Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) (IETF RFC 3605:2003)
- DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6) (IETF RFC 3646:2003)
- Extensions to FTP (IETF RFC 3659:2007)
- Collective Attributes in LDAP (IETF RFC 3671:2003)
- Subentries in LDAP (IETF RFC 3672:2003)

- LDAPv3: All Operational Attributes (IETF RFC 3673:2003)
- LDAP Component Matching Rules (IETF RFC 3687:2004)
- LDAP: Additional Matching Rules (IETF RFC 3698:2004)
- Stream Control Transmission Protocol (SCTP) Partial Reliability Extension (IETF RFC 3758:2004)
- Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents (IETF RFC 3776:2004)
- Multicast Listener Discovery Version 2 (MLDv2) for IPv6 (IETF RFC 3810:2004)
- Stream Control Transmission Protocol (SCTP) Management Information Base (MIB) (IETF RFC 3873:2004)
- Network Information Service (NIS) Configuration Options for DHCPv6 (IETF RFC 3898:2004)
- LDAP Cancel Operation (IETF RFC 3909:2004)
- Border Gateway Multicast Protocol (BGMP) (IETF RFC 3913:2004)
- LDAP Client Update Protocol (IETF RFC 3928:2004)
- Internet Low Bit Rate Codec (iLBC) (IETF RFC 3951:2004)
- Real-time Transport Protocol (RTP) Payload Format for internet Low Bit Rate Codec (iLBC) Speech (IETF RFC 3952:2004)
- Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address (IETF RFC 3956:2004)
- Protocol Independent Multicasting Dense Mode (PIM-DM) (IETF RFC 3973:2005)
- Network News Transfer Protocol (NNTP) (IETF RFC 3977:2006)
- IPv6 Scoped Address Architecture (IETF RFC 4007:2005)
- Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE) (IETF RFC 4023:2005)
- A Method for Storing IPsec Keying Material in DNS (IETF RFC 4025:2005)
- Provider Provisioned Virtual Private Network (VPN) Terminology (IETF RFC 4026:2005)
- Scenarios and Analysis for Introducing IPv6 into ISP Networks (IETF RFC 4029:2005)
- The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option (IETF RFC 4030:2005)
- Service Requirements for Layer 3 Provider Provisioned Virtual Private Networks (PPVPNs) (IETF RFC 4031:2005)
- Update to the Session Initiation Protocol (SIP) Preconditions Framework (IETF RFC 4032:2005)
- IP Authentication Header (AH) (IETF RFC 4302:2005)
- LDAP Proxied Authorisation Control (IETF RFC 4370:2006)
- LDAP Bulk Update Replication Protocol (LBURP) (IETF RFC 4373:2006)
- LDAP Schema for UDDI (IETF RFC 4403:2006)
- Lightweight Directory Access Protocol (LDAP) - Binary Encoding Option (IETF RFC 4522:2006)
- Lightweight Directory Access Protocol (LDAP) - COSINE Schema (IETF RFC 4524:2006)
- Lightweight Directory Access Protocol (LDAP) - Modify-Increment Extension (IETF RFC 4525:2006)
- Lightweight Directory Access Protocol (LDAP) - Absolute True and False Filters (IETF RFC 4526:2006)

- Lightweight Directory Access Protocol (LDAP) - Read Entry Controls (IETF RFC 4527:2006)
- Lightweight Directory Access Protocol (LDAP) - Assertion Control (IETF RFC 4528:2006)
- Lightweight Directory Access Protocol (LDAP) - Requesting Attributes by Object Class (IETF RFC 4529:2006)
- Lightweight Directory Access Protocol (LDAP) - entryUUID (IETF RFC 4530:2006)
- LDAP Turn Operation (IETF RFC 4531:2006)
- Lightweight Directory Access Protocol (LDAP) Who am I? Operation (IETF RFC 4532:2006)
- Lightweight Directory Access Protocol (LDAP) Content Sync Operation (IETF RFC 4533:2006)
- Considerations for Internet group Management protocols (IGMP) and Multicast listener Discovery Snooping Switches (IETF RFC 4541:2006)
- OSPF version 2 Management Information Base:2006 (IETF RFC 4750:2006)
- IPv6 over Low Power Wireless Personal Area Networks (IETF RFC 4919:2007)
- Multicast Group Membership Discovery MIB (IETF RFC 5519:2009)
- Mobile IPv6 Support for Dual Stack Hosts and Routers (IETF RFC 5555:2009)
- Mobile IPv6 Fast Handovers (IETF RFC 5568:2009)
- Extended MKCOL for Web Distributed Authoring and Versioning (WebDAV) (IETF RFC 5689:2009)
- FTP Command and Extension Registry (IETF RFC 5797:2010)
- Registration of Military Message Handling System (MMHS) Header Fields for Use in Internet Mail (IETF RFC 6477:2012)
- Simplified Multicast Forwarding (SMF) (IETF RFC 6621:2012)
- Multicast DNS (IETF RFC 6762:2013)
- DNS-Based Service Discovery (IETF RFC 6763:2013)
- Update to Internet Message Format to Allow Group Syntax in the From: and Sender: Header Fields (IETF RFC 6854:2013)
- File Transfer Protocol HOST Command for Virtual Hosts (IETF RFC 7151:2014)

D.2.5. ISACA

- COBIT 5: A Business Framework for the Governance and Management of Enterprise IT (ISACA Cobit 5:2012)

D.2.6. ISO/IEC

- Systems and software Quality Requirements and Evaluation (SQuaRE) - Evaluation process (ISO/IEC 2540-1:2011)
- Information technology - Document description and processing languages - HyperText Markup Language (HTML) (ISO/IEC 15455:2000)
- Information Technology - Cloud Computing - Interoperability and Portability (ISO/IEC 19941:2017)
- Information technology - Distributed Application Platforms and Services (DAPS) - General technical principles of Service Oriented Architecture (ISO/IEC 30102:2012)

- Keyboard Layouts Part 1: General principles governing keyboard layouts (ISO/IEC 9995-1:2009)
- Keyboard Layouts Part 2: Alphanumeric section (ISO/IEC 9995-2:2009)
- Keyboard Layouts Part 3: Complementary layouts of the alphanumeric zone of the alphanumeric section (ISO/IEC 9995-3:2010)
- Keyboard Layouts Part 4: Numeric section (ISO/IEC 9995-4:2009)
- Keyboard Layouts Part 5: Editing and function section (ISO/IEC 9995-5:2009)
- Keyboard Layouts Part 6: Function section (ISO/IEC 9995-6:1994)
- Keyboard Layouts Part 7: Symbols used to represent functions (ISO/IEC 9995-7:2009)
- Keyboard Layouts Part 8: Allocation of letters to the keys of a numeric keypad (ISO/IEC 9995-8:2009)
- Volume and file structure of CD-ROM for information interchange (ISO/IEC DIS 9660:1988)
- Generic coding of moving pictures and associated audio information -- Part 5: Software simulation (ISO/IEC TR 13818-5:2005)

D.2.7. ITU-T

- 14 kHz audio codec (ITU-T G.722.1c:2012)

D.2.8. MIL-STD

- Connectors, Fiber Optic, Circular, Environmental Resistant, Hermaphroditic, General Specification for. D (MIL-STD DTL 83526:2006)

D.2.9. MIP

- MIP Information Model 5.0 (MIP MIM 5.0:2019)

D.2.10. Microsoft

- Rich Text Format (RTF) Specification, Version 1.9.1 (Microsoft RTF 1.9.1:2008)

D.2.11. NATO

- VLF / LF MSK Multi Channel Broadcast (NATO AComP-4724 Ed A Ver 1:2015)
- Concept of NATO Message Text Formatting System (CONFORMETS) (NATO ADatP-03 Ed A Ver 3:2019)
- Imagery Air Reconnaissance Tape Recorder Interface (NATO AEDP-11 Ed 1:2001)
- Tactical Data Exchange - Link 1 (Point-to-Point) (NATO ATDLP-5.01 Ed A Ver 1:2015)
- Materiel Configuration Management Policy and Procedures for Multinational Joint Projects, edition 2 (NATO STANAG 4159 Ed 2:1991)
- Standards to Achieve Communication Between Single Channel Tactical Combat Net Radio Equipment and Frequency Hopping Radios Operating in the same VHF (30-108 MHz) Band (NATO STANAG 4292 Ed 2:1987)

- Navstar Global Positioning System (GPS)(PART I) Summary Of Performance Requirements (NATO STANAG 4294 Ed 2 Part 1:1997)
- Interoperability of Low-level Ground-based Air Defence Surveillance, Command and Control Systems (NATO STANAG 4312 Ed 2:2012)
- VLF / LF MSK Multi Channel Broadcast - AComP-4724 Edition A (NATO STANAG 4724 Ed 1:2015)
- Standard for Interconnection of IPv4 Networks at Mission Secret and Unclassified Security Levels (NATO STANAG 5067 Ed 1:2015)
- Tactical Data Exchange - Link 11/11B (NATO STANAG 5511 Ed 6:2008)
- Tactical Data Exchange - Link 16 (NATO STANAG 5516 (RD) Ed 5:2009)
- NATO Improved Link Eleven (NILE) - Link 22 (NATO STANAG 5522 Ed 2:2008)
- Tactical Data Link - Link 22 (NATO STANAG 5522 (RD) Ed 3:2009)
- Standard Data Elements (SDE) (NATO STANAG 5526 Ed 1)
- Imagery Air Reconnaissance Tape Recorder Interface - AEDP-11 Edition 1 (NATO STANAG 7024 Ed 2:2001)

D.2.12. NATO Study (expected)

- Link-22 (NATO Study (expected) STANAG 5522 Ed 4)
- Link-22 - ATDLP-5.22 Edition A (NATO Study (expected) STANAG 5522 Ed 5)

D.2.13. OGC

- Web Coverage Service Implementation Standard v1.1.2 (OGC 07-067r5:2008)

D.2.14. US DoN

- Operational Specification for OVER-THE-HORIZON TARGETING GOLD (Revision C) (OTH-G) (US DoN OTH-G Rev C:1997)

D.2.15. USB.ORG

- Wireless USB Specification (USB.ORG Wireless Specification:2005)

APPENDIX E. PROCESSED RFCS

101. The following RFC have been processed::

RFC #	Title	Origin
11-004	Remove STANAG 5067 Ed 1	NCIA
14-001a	Replace STANAG 5511 Ed 4 with ATDLP 5.11 Ed. B Ver 1 in BSP	TDL
14-001b	Replace STANAG 5516 Ed 4 with ATDLP 5.16 Ed. B Ver 1 in BSP	TDL
14-001c	Replace STANAG 5518 Ed 1 with ATDLP 5.18 Ed. B Ver 2 in BSP	TDL
14-001d	Update ATDLP-5.01 Ed A Ver 1 to ATDLP-5.01 Ed A Ver 2 in the BSP	TDL
14-001e	Remove ATDLP-7.03 Ed B Ver 1 from NISP BSSP for Informal_Messaging_Services	TDL
14-002	For all AEP-76 standards: change RP to LCGDSS and harmonize all publications numbers.	NHQ/CNAD
14-003	Remove STANAG 4312 Ed 2	CNAD
14-004	Remove STANAG 4292 Ed 2	LOS Comms CaT
14-005	Update ADatP-03 Ed A Ver 3 to ADatP-03 Ed A Ver 4	MTF CaT
14-006	Remove CIM, DSP 004, DSP 0226, DSP 0227, DSP 0252 & CIM Schema	SMC CaT
14-007a	Add AGeoP-26 Ed B Ver 1 as candidate standard in Geospatial Services	GRWG/JGSWG
14-012	CaP 2/FFT WG and CaP 2/IFF WG replaced as RP with CaP 2	CaP 2
14-013	Add Joint Domain Service and related standards to the BSP	CaP 2
14-015	Move emerging STANAG 4722 from Track Management Services to Air Domain	CaP 4
14-016	Add ANP-4564 Ed S Ver 1 / STANAG 4564 Ed 3 Maritime Domain Services	CaP 4
14-018	Move AEtP-4579 Ed A Ver 1 / STANAG 4579 Ed 2 from Track Management Systems to Land Domain Services.	CaP 2
14-019	Move STANAG 4162 Ed 2 from Track Management Services to Recognized Picture Services	CaP 2
14-020	Remove reference to non existing paragraph.	TDL

RFC #	Title	Origin
14-027a	Replace in cryptographic services the profile TN-1491 Ed 2 Annex A with ADatP-4778.2 Edition A Version 1 Chapter 2	NCIA
14-027b	Replace in informal messaging services the profile TN-1491 Ed 2 Annex B with ADatP-4778.2 Edition A Version 1 Chapter 2	NCIA
14-027c	Replace in informal messaging services the profile TN-1491 Ed 2 Annex C with ADatP-4778.2 Edition A Version 1 Chapter 4	NCIA
14-027d	Replace in informal messaging services the profile TN-1491 Ed 2 Annex D with ADatP-4778.2 Edition A Version 1 Chapter 5	NCIA
14-027e	Replace in informal messaging services the profile TN-1491 Ed 2 Annex E with ADatP-4778.2 Edition A Version 1 Chapter 6	NCIA
14-027f	Replace in informal messaging services the profile TN-1491 Ed 2 Annex F with ADatP-4778.2 Edition A Version 1 Chapter 7	NCIA
14-027g	Replace in informal messaging services the profile TN-1491 Ed 2 Annex G with ADatP-4778.2 Edition A Version 1 Chapter 8	NCIA
14-027h	Replace in informal messaging services the profile TN-1491 Ed 2 Annex H with ADatP-4778.2 Edition A Version 1 Chapter 9	NCIA
14-027i	Replace in informal messaging services the profile TN-1491 Ed 2 Annex I with ADatP-4778.2 Edition A Version 1 Chapter 10	NCIA
14-027j	Replace in informal messaging services the profile TN-1491 Ed 2 Annex J with ADatP-4778.2 Edition A Version 1 Chapter 11	NCIA
14-027k	Replace in informal messaging services the profile TN-1491 Ed 2 Annex K with ADatP-4778.2 Edition A Version 1 Chapter 12	NCIA
14-028a	Remove ATDLP 5.11 Ed B Ver 1 in volume 3 from Track Management, Formal messaging, Communication Access and Tactical Messages	TDL
14-028d	Replace the standard STANAG 5522 with ATDLP 5.22 Edition B Version 1	TDL

RFC #	Title	Origin
14-028e	Replace the standard STANAG 5616ed5 with ATDLP 6.16 (vol I,II,II and IV) Edition B Version 1	TDL
14-028h	Replace ATDLP 5.16 Ed B / STANAG 5516 Ed 8 with ATDLP 5.16 Ed C / STANAG 5516 Ed 9 in volume 3	TDL
14-028i	Replace ATDLP 5.18 Ed B Ver 2 / STANAG 5518 Ed 4 with ATDLP 5.18 Ed C Ver 1 / STANAG 5518 Ed 5 in volume 3	TDL
14-030	Add ADatP-37 in the BSP Track Distribution Service in volume 2	CaP 2
14-031	Replace STANAG 4294 ed 2 with STANAG 4294 ed 3	CaP 2
14-032	Add FMN Spiral 5	ACT
14-057	Replace ATP-97 Ed A with ATP-97 Ed B with SLIERP as responsible party	MCLSB SLIERP
14-058	Add ATP-105 Ed A with SLIERP as responsible party	MCLSB SLIERP
14-060	Delete obsolete standards	NCIA
14-061	Remove obsolete IETF RFCs from the BSP	NCIA
14-062	Extensive quality review of the NISP database	IP CaT
14-063	Remove mil-dtc83526, which is a duplicate of mil-dtc-83526c	IP CaT
14-065	Change publicationnumber for NATO standard AComp-4787 Ed A Ver 1	IP CaT
14-066	Add STANAG 1459 ED 3	IP CaT
14-067	NISP Scrubbing - Correction	IP CaT
14-068	Update C3 Taxonomy to version 5	IP CaT
14-069	Undelete a bunch of standards, because they are used in FMN Spiral 4	IP CaT
14-070	Add Service Interface Profile for Geospatial Services – Geoprocessing Services	NCIA
14-071	Change responsible party for OTH-Gold to FMN CPWG	DM CaT
14-072	Update MIM from ver 5.0 to 5.1	DM CaT
14-073	Clean-up of data	IP CaT
14-074	Clean-up OTH-T Gold meta-data	IP CaT
14-075	Reference Change to MIP4 IES	DM CaT

This page is intentionally left blank

APPENDIX F. ARCHIMATE EXCHANGE FORMAT

102. The C3B have tasked IP CaT to improve the consistency and usability of NISP. IP CaT have therefore in "A standard representation and exchange specification for Interoperability Standards and Profiles" ver 0.8 dated Dec 10, 2020 (AC-322-WP(2020)0036) specified a semantic representation of the data set contained in the NISP as an architecture model in the Open Group ArchiMate Modelling Language so that this model can be exchanged via the ArchiMate Model Exchange File Format Standard between tools and/or systems that can import, and export ArchiMate models. ArchiMate Exchange Files enable exporting content from one ArchiMate modelling tool or repository and importing it into another while retaining information describing the model in the file and how it is structured, such as a list of model elements and relationships. Extensions of ArchiMate are specified in accordance with the Language Customization Mechanisms and where possible re-use metadata elements defined by the NATO Core Metadata Specification (NCMS)to limit the definition of NISP specific metadata requirements.

This page is intentionally left blank