NATO STANDARD

ADatP-34(L) / Version 12

NATO Interoperability Standards and Profiles

Volume 1

Introduction

19 Jul 2019

Allied Data Publication

Table of Contents

List of Figures

This page is intentionally left blank

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(L) when approved by the C3 Board[1].

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 recommended non-NATO[2] 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)
CIS	Communication and Information Systems

[1] AC/322-N(2019)0052-REV1-COR-1 approved ADatP-34(L)
[2] ISO or other recognized non-NATO standards organization

Abbreviation	Full Text
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 Definition is to be found in EAPC(AC/322)D (2006)0002-REV 1): 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. Note: A service interoperability point 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	Service Interface Profile
SME	Subject Matter Expert

Abbreviation	Full Text
SOA	Service Oriented Architecture
STANAG	NATO abbreviation for **STAN**dardization **AG**reement, which set up processes, procedures, terms, and conditions for common military or technical procedures or equipment between the member countries of the alliance.
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(2014)0016) all NATO Enterprise (ref. C-M(2014)0061) entities shall adhere to the NISP mandatory standards and profiles in volume 2.

008. Other activities that assure interoperability within the alliance should list their profiles in the NISP.

1.2. INTENDED AUDIENCE

009. 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.

010. 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

011. 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 in 2019.

This page is intentionally left blank

CHAPTER 2. BASIC CONCEPTS

012. This chapter gives an overview to understand the data in volume 2 and volume 3.

2.1. STANDARDS

013. Standards (their content) are defined and managed in their life cycle by standardization bodies with their own timetable. A standard may have 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. For aspects of obligation status for standards in planning and programmes, see the next paragraph.

2.2. STANAG

014. STANAG's are managed by the NATO Standardization Office (NSO). NATO STANAG's that are promulgated shall be considered mandatory only for NATO common-funded systems. If NISP references a STANAG, the obligation status for it is only informative. The NSO maintains the obligation status in their own process of standardization.

015. Some older STANAG's combine the agreement and the actual specification into one single document. NISP references the specification part.

016. Some STANAG's and NATO Standards included in the NISP are not yet registered in the NSO database. To indicate this, in the NISP tables the publication number starts with "NSO-Expected" instead of "NSO" and in the index, they are grouped under "NATO Standardization Office (expected in the future)".

017. For some STANAG's, the status in the NISP deviates from the status according to the NSO. For example, the NISP contains mandatory STANAGs that are Superseded or Cancelled according to the NSO. Also the NISP contains candidate STANAGs that are already Promulgated according to the NSO. For those STANAG's, this deviation is documented in a footnote.

018. When a STANAG is not yet Promulgated, this is identified by including "Study" or "RD" (Ratification Draft) in the publication number.

2.3. INTEROPERABILITY PROFILES

019. Profiles define the specific use of standards at a service interoperability point (SIOP) in a given context. Profiles support prerequisites for programmes or projects and enable interoperability implementation and testing.

020. 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.

021. 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. NATO STANAGS's that are promulgated shall be considered mandatory. 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.

022. 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.

023. 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.

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

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

2.4. BASIC STANDARDS PROFILE

026. 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.

027. 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).

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

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

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

2.5.1. Architecture Building Block

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

2.5.1.1. Characteristics

031. ABBs:

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

2.5.1.2. Specification Content

032. 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

2.5.2. FMN Spiral Specifications

033. 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".

034. 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.

2.5.3. Capability Packages

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

CHAPTER 3. ORGANIZATION OF THE NISP INFORMATION

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

3.1. NISP STRUCTURE

037. 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.

038. 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

039. 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(2019)0037
Alliance C3 Policy (25 April 2016)	C-M(2015)0041-REV1
NATO Defence Planning Process (NDPP)	PO(2016)0655 (INV)

040. 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.

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

042. 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

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

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

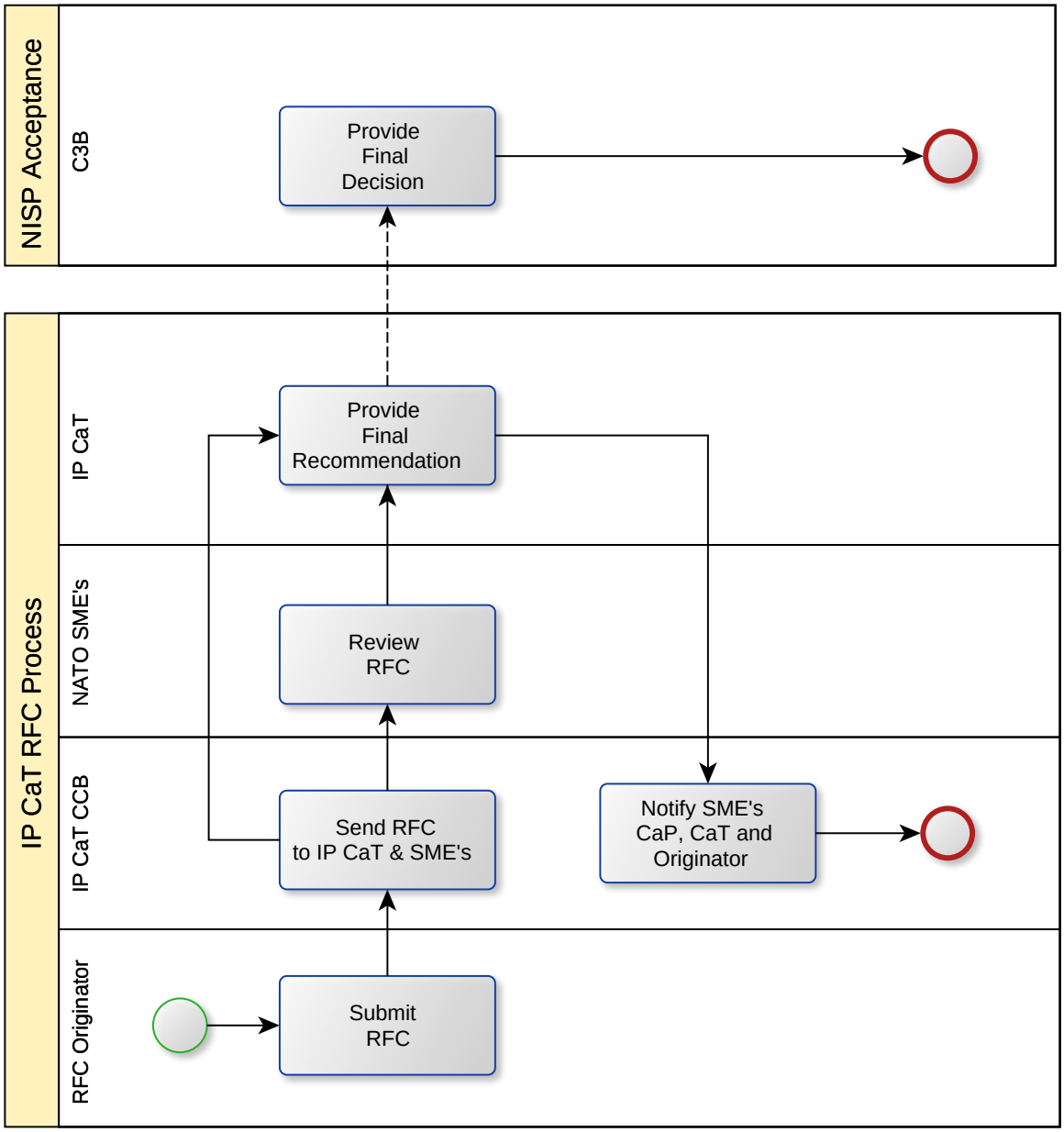

Figure 5.1. RFC Handling Process

045. 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:

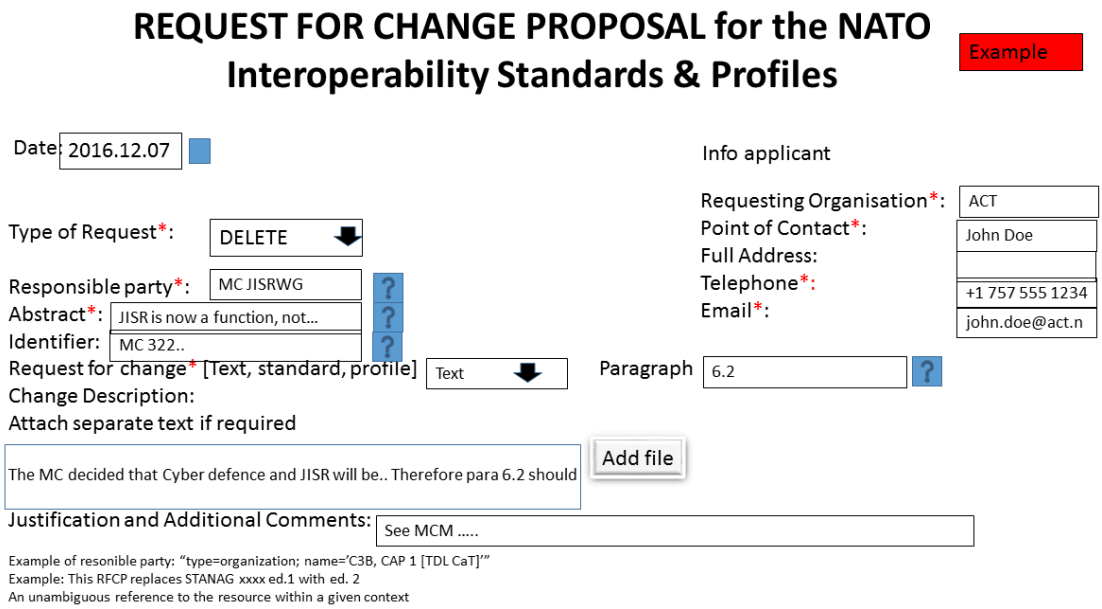

Figure 5.2. RFC Notional Form

046. 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.

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

048. 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

049. 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.

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

5.2. NISP PRODUCTS

051. The NISP is published in several formats:

- Documentation in HTML and PDF Formats
- Website and searchable online Database
- Data export in XML format

This page is intentionally left blank

CHAPTER 6. NATIONAL SYSTEMS INTEROPERABILITY COORDINATION

052. 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.

053. 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 Edition 2. 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

054. 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.

055. 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].

056. The NISP organizes the standards using the structure of the latest approved baseline of NATO's C3 Taxonomy. 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/tidepedia/index.php/C3_Taxonomy. 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 recommended 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

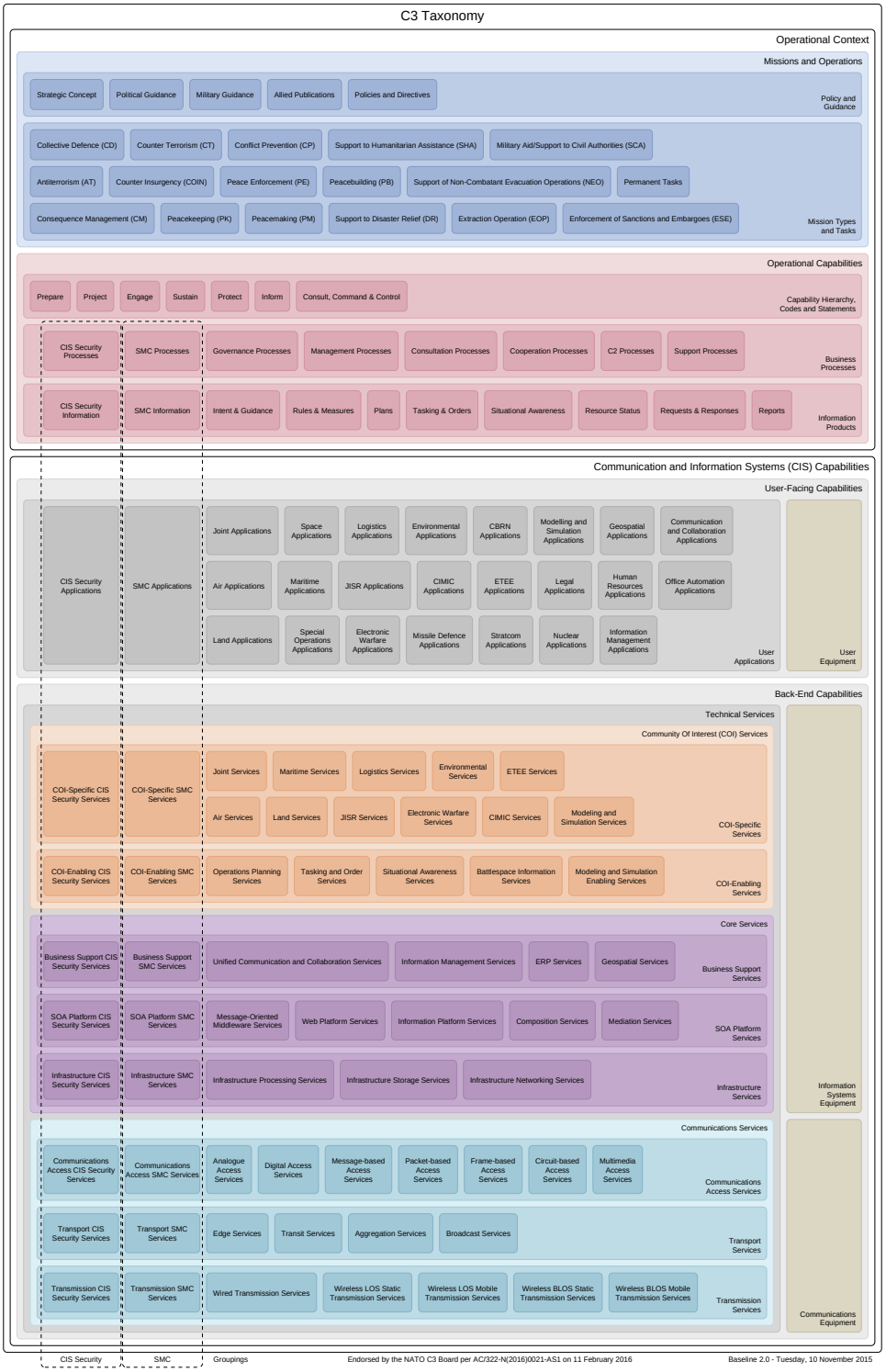

Figure 7.1. C3 Taxonomy

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

058. 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

059. 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

060. 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.

061. 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.

062. 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

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

064. 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.

065. 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

066. 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.

067. 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

068. 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

069. 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.

070. 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

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

A.5.1. Identification

072. 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

073. 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.

074. 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

075. 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

076. 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

077. 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).

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

079. 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

080. 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

081. 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)

082. 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

083. 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

084. 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

085. 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

086. 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

087. 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.

088. 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.

089. 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.

090. 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.

091. 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, 26 January 2016 and SHAPE/PLANS/JCAP/FCP/16-311533 5000/FPR-0460/TTE-151451/Ser:NU0083
[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.

092. 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.

093. 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 FROM NISP VERSION 11 (K) TO NISP VERSION 12 (L)

094. Major content changes to NISP v12 include:

- FMN Spiral 3 Profile added as Mandatory (Vol 2)
- 13 RFCs processed. Details of the RFC changes are captured in Appendix E.

This page is intentionally left blank

APPENDIX D. DETAILED CHANGES FROM NISP VERSION 11 (K) TO NISP VERSION 12 (L)

D.1. NEW STANDARDS

D.1.1. C3B

- CIS Security Technical and Implementation Directive on Cryptographic Security and Mechanisms for the Protection of NATO Information within NNN & IO CIS (C3B AC/322-D(2015)0031:2015)

D.1.2. C3B TDL CaT

- Interface Control Definiton for the International Exchange of MIDS/JTIDS Network (NETMAN T/1) (C3B TDL CaT ATDLP-7.03(B)(1))

D.1.3. CIS3 C&IP

- Securing SIP Signaling - Use of TLS with SCIP (CIS3 C&IP SCIP-214.3:2014)
- X.509 Elliptic Curve (EC) Key Material Format Specification (CIS3 C&IP SCIP-233.109:2014)

D.1.4. IEEE

- IEEE Standard for Ethernet (IEEE 802.3:2018)

D.1.5. IETF

- Transport Layer Security Protocol Compression Methods (IETF RFC 3749:2004)
- The Transport Layer Security (TLS) Protocol Version 1.1 (IETF RFC 4346:2006)
- Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) (IETF RFC 4492:2006)
- Internet Calendaring and Scheduling Core Object Specification (iCalendar) (IETF RFC 5545:2009)
- iCalendar Transport-Independent Interoperability Protocol (iTIP) (IETF RFC 5546:2009)
- Transport Layer Security (TLS) Renegotiation Indication Extension (IETF RFC 5746:2010)
- iCalendar Message-Based Interoperability Protocol (iMIP) (IETF RFC 6047:2010)
- Transport Layer Security (TLS) Extensions: Extension Definitions (IETF RFC 6066:2011)
- The Secure Sockets Layer (SSL) Protocol Version 3.0 (IETF RFC 6101:2011)
- Prohibiting Secure Sockets Layer (SSL) Version 2.0 (IETF RFC 6176:2011)
- Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension (IETF RFC 6520:2012)

- The Transport Layer Security (TLS) Multiple Certificate Status Request Extension (IETF RFC 6961:2013)
- Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content (IETF RFC 7231:2014)
- Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests (IETF RFC 7232:2014)
- Hypertext Transfer Protocol (HTTP/1.1): Range Requests (IETF RFC 7233:2014)
- Hypertext Transfer Protocol (HTTP/1.1): Caching (IETF RFC 7234:2014)
- Hypertext Transfer Protocol (HTTP/1.1): Authentication (IETF RFC 7235:2014)
- Encrypt-then-MAC for Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) (IETF RFC 7366:2014)
- Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) (IETF RFC 7525:2015)
- Deprecating Secure Sockets Layer Version 3.0 (IETF RFC 7568:2015)
- Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension (IETF RFC 7627:2015)
- Transmission Control Protocol (IETF RFC 793:1981)
- The SSL Protocol (IETF RFC SSL2:1995)

D.1.6. ISO

- Document management -- Portable document format -- Part 2: PDF 2.0 (ISO 32000-2:2017)

D.1.7. ISO/IEC

- Information technology -- Generic cabling for customer premises -- Part 1: General requirements (ISO/IEC 11801-1:2017)

D.1.8. MIL-STD

- Connectors, fiber optic, circular, environmental resistant, hermaphroditic, general specification for (MIL-STD DTL 83526 Rev D:2014)

D.1.9. NIST

- Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography (NIST SP 800-56A Rev 3:2018)

D.1.10. NSA

- CSfC Multi-Site Connectivity Capability Package (NSA :2017)

D.1.11. NSO

- Captured Persons, Materiel And Documents - AJP-2.5(A) (NSO STANAG 2195 Ed 2:2007)
- Allied Joint Medical Doctrine For Medical Evacuation - AJMedP-2 Edition A (NSO STANAG 2546 Ed 2:2018)

- NATO Land Urgent Voice Messages (LUVM) Pocket Book - ATP-97 Edition A (NSO STANAG 2627 Ed 1:2016)
- Technical standards for single channel UHF radio equipment (NSO STANAG 4205 Ed 4:2018)
- NATO Intelligence, Surveillance And Reconnaissance Tracking Standard – AEDP-12 Edition A (NSO STANAG 4676 Ed 1:2014)
- NATO standardization of measurement and signature intelligence (MASINT) Reporting - AEDP-16 Edition A (NSO STANAG (Study) 4716 Ed 1)
- NATO Vector Graphics (NVG) 2.0.2 - ADatP-4733 Edition A Ver 1 (ADatP-4733 Ed A Ver 1:2014)

D.1.12. NSO-Expected

- Multi-Link Standard Operating Procedures for Tactical Data Systems Employing Link 11, Link 11B, Link 16, Link 22 and JREAP (NSO-Expected ATDLP-7.33(B)(1))
- Standard for Joint Range Extension Application Protocol (JREAP) - ATDLP-5.18 Edition B (NSO-Expected STANAG (RD) 5518 Ed 4 / ATDLP-5.18(B)2:2016)

D.1.13. TM-FORUM

- TMF000 Event API REST Specification R17.5 (TM-FORUM TMF000:2017)
- TMF630 API Design Guidelines 3.0 R17.5.0 (TM-FORUM TMF630:2017)
- TMF638 Service Inventory API REST Specification R16.5 (TM-FORUM TMF638:2016)
- TMF641 Service Ordering API REST Specification R16.5.1 (TM-FORUM TMF641:2017)
- TMF661 Trouble Ticket API Conformance Profile R16.5.1 (TM-FORUM TMF661:2017)

D.1.14. US DoD

- Variable Message Format (VMF) (US DoD MIL-STD-6017 D:2017)

D.1.15. W3C

- Geolocation API Specification 2nd Edition (W3C geolocation-API:2016)
- HTML5 Differences from HTML4 (W3C NOTE-html5-diff:2014)
- Hypertext Markup Language revision 5.2 (HTML5) (W3C REC-html52:2017)
- Hypertext Markup Language revision 5.3 Editor's Draft (4.7) (W3C REC-html53-Draft:2018)
- Media Source Extensions (W3C REC-media-source:2016)
- Mobile Web Application Best Practices (W3C REC-mwabp:2010)
- Web Speech API (W3C speech-API:2018)
- DOM Parsing and Serialization (W3C WD-DOM-Parsing:2016)

D.1.16. XMPP

- XEP-0220: Server Dialback (XMPP XEP-0220:2014)

D.2. DELETED STANDARDS

D.2.1. DMTF

- Configuration Management Database (CMDB) Federation Specification (DMTF DSP0252:2009)

D.2.2. ECMA

- Office Open XML (ECMA ECMA-376:2008)

D.2.3. ESRI

- Esri Open GeoServices REST Specification, v.1.0 (ESRI REST:2010)
- ESRI Shapefile Technical Description (ESRI shapefile:1998)

D.2.4. GDAL

- Geospatial Data Abstraction Library (GDAL) (GDAL gdal:2013)

D.2.5. IETF

- The Kerberos Network Authentication Service (V5) (IETF RFC 1510:1993)
- Internet Protocol, version 6 (IETF RFC 2460:1998)

D.2.6. NSO-Expected

- NATO TDL Implementation Plan (NTDLIP T/1) (NSO-Expected NTDLIP Rev.3)

D.2.7. US DoD

- Common Warfighting Symbology (US DoD MIL-STD 2525B:1999)
- Common Warfighting Symbology (US DoD MIL-STD-2525C:2008)

D.3. DETAILED CHANGES

095. The previous two sections explicitly list added and deleted standards since the latest release of NISP. The enclosed spreadsheet lists all changes, such as added and deleted standards, but also how standards have been added, deleted and moved within profiles.

APPENDIX E. PROCESSED RFCS

096. The following RFC have been processed::

RFC #	Title	Origin
11-002	Remove SIP template	NCIA
11-005	Add set of HTTP standards: RFC 7231-7235	NCIA
11-008	Update biometric specs	NCIA
11-011	Update standards in military message services	DEU
11-014	Update definition of a Candidate, so unapproved standards can temporary be part of volume 3	GRC
11-015	Add reference to a Congnitive Computing service	ACT
11-019	Update STANAG 4559	USA
11-052	Remove remaining elements of the AMN profile	IP CaT
11-053	Transfer responsibility for AMN standard which shoud be kept to SM CaT	IP CaT
11-054	Transfer responsibility for AMN standard which shoud be kept to JCGISR	IP CaT
11-055	Transfer responsibility for AMN standard which shoud be kept to C3B CaP 1	IP CaT
11-056	Update MIL STANDARD 6017 to edition D	US Mission to NATO
11-057	Add FMN Spiral 3 as mandatory profile	CPWG

This page is intentionally left blank