20 April 2021

DOCUMENT
AC/322-D(2019)0041-REV1

CONSULTATION, COMMAND AND CONTROL BOARD (C3B)

Technical and Implementation Directive on Introducing Secure Systems and Solutions Using Commercial-Off-the-Shelf (COTS) Products into NATO

Note by the Secretary

Reference:

A. AC/322-WP(2020)0034-REV1-AS1, 30 Mar 21.

1. On 25 Mar 21, the C3B approved the Revision of the NATO Information Assurance Product Catalogue (NIAPC) Appendix (Reference A).

2. Enclosed is the updated version of the Technical and Implementation Directive on Introducing Secure Systems and Solutions Using Commercial-Off-the-Shelf (COTS) Products into NATO, now including the agreed NIAPC appendix.

3. With the inclusion of the NIAPC appendix, this revised version also supersedes the previous NIAPC directive (Reference AC/322-D(2010)0042, 22 Sep 10).

(Signed) S. Ndagijimana-Munezero

Action Officer: Mrs.J.Arthur, ext. 5385
Original: English

Annex 1: Technical and Implementation Directive on Introducing Secure Systems and Solutions Using Commercial Off The Shelf (COTS) Products into NATO

1 Annex

ANNEX1
AC/322-D(2019)0041-REV1

Technical and Implementation Directive on Introducing Secure Systems and Solutions Using Commercial Off The Shelf (COTS) Products into NATO

Contents

References:

A. C-M(2007)0118, NATO Information Management Policy (NIMP), 11 Dec 2007

B. C-M(2002)49-REV1, Security within the North Atlantic Treaty Organization, 20 Nov 2020

C. C-M(2011)0042, NATO Policy on Cyber Defence, 7 Jun 2011

D. C-M(2002)60, Management of Non-Classified NATO Information, 11 Jul 2002

E. AC/35-D/2004-REV3, Primary Directive on CIS Security, 15 Nov 2013

F. AC/35-D/2005-REV3, Management Directive on CIS Security, 12 Oct 2015

G. AC/35-D/1021-REV3, Guidelines for the Security Accreditation of Communication and Information Systems (CIS), 31 Jan 2012

H. AC/322-D/0047-REV2 (INV), INFOSEC Technical & Implementation Directive on Cryptographic Security and Cryptographic Mechanisms, 11 Mar 2009

I. AC/322-D(2004)0030, INFOSEC Technical & Implementation Directive on the Requirement for, and the Selection, Approval and Implementation of, Security Tools, 17 May 2004

J. AC/322-D/0048-REV3, Technical and Implementation Directive on CIS Security, 18 Nov 2019

K. AC/322-D/0030-REV5, INFOSEC Technical and Implementation Directive for the Interconnection of Communication and Information Systems (CIS), 23 Feb 2011 (under revision).

L. AC/322-D(2006)0041-REV2, Directive on the Selection and Procurement of NATO Common-Funded Cryptographic Systems, Products, and Mechanisms, 8 July 2009.

M. AC/322-D(2019)0041, Technical & Implementation Directive on Introducing Secure Systems and Solutions Using Commercial Off The Shelf (COTS) Products into NATO, 1 Oct 2019

N. AC/322-D(2017)0016 (INV), Technical & Implementation Directive on NATO Supply Chain Security Requirements for CIS Security Enforcing Products, March 2017

O. SDIP-27/2, NATO TEMPEST Requirements and Evaluation Procedures, 4 May 2016

P. SDIP-55, NATO TEMPEST Vendor Qualification and Control, 2 Sep 2010

1. Foreword

This Directive specifies the requirements to be satisfied when COTS products with security enforcing functionality are procured for use within NATO. It encompasses a variety of mechanisms for gaining the necessary assurance and outlines relevant elements of the specification and procurement lifecycle.

2. Introduction

Many Communication and Information Systems (CIS), services, and individual products used by NATO must enforce aspects of security. To provide this in a cost effective manner requires an appropriate blend of architectural design, assured product functionality, and operational monitoring. Cost effective product security assurance should reuse as much evidence as possible, particularly where a product has already been evaluated as part of a certification or approval scheme, so that NATO funded evaluation can be targeted on essential areas (e.g. higher level of cryptography following Strength of Mechanism (SoM) levels as specified by Reference H). Recognition arrangements that minimize duplication of evaluation activities can therefore be highly beneficial.

2.2. Directive

This CIS Security Technical and Implementation Directive is published by the C3 Board in support of the Primary Directive on CIS Security (Reference E) and the following policies, for the protection of classified and non-classified information:

1. NATO Information Management Policy (NIMP) (Reference A),
2. Security within the North Atlantic Treaty Organization (Reference B) and
3. The Management of Non-Classified NATO Information (Reference D).

2.3. Purpose

This Directive expresses the requirements that are to be satisfied when Commercial- Off-The-Shelf (COTS) security enforcing products are procured for use within NATO. It complements the Management Directive on CIS Security (Reference F), which explains why certain categories of security enforcing products shall be security evaluated for any CIS implementation. This Directive is to be read in conjunction with relevant NATO policies (References A through D) and supporting directives, including policy and minimum standards for the protection of CIS handling NATO non-classified information (Reference E)[1], the Primary Directive on CIS Security, and the CIS Security Directives.

[1] AC/35-D/2020 (INV), Directive on the Protection of CIS Handling Non-classified NATO Information, 6 Nov 2019

2.4. Scope

This Directive applies to all NATO Communication and Information Systems (CIS) storing, processing, or transmitting NATO information where a security accreditation is required. It covers the procurement of products to be integrated into systems (e.g., firewalls, virtual private network gateways) or procured for a broader NATO use case (e.g., mobile devices, USB portable storage devices). As such, only the Electronic Security Environment (ESE) aspects are covered in this directive, other directives address the Global Security Environment (GSE) and the Local Security Environment (LSE).

The selection, evaluation and approval of cryptographic mechanisms, used by confidentiality and non-confidentiality services for the protection of classified information, is not covered by this directive. Such cryptographic mechanisms are selected, evaluated and approved following the requirement for Strength of Mechanism (SoM) as laid out in the INFOSEC Technical & Implementation Directive on Cryptographic Security and Cryptographic Mechanisms (Reference H and L).

This Directive applies to authorities that are responsible for establishing and implementing CIS security requirements and for ensuring that CIS security measures are maintained. This includes Security Accreditation Authorities, CIS Planning and Implementation Authorities, CIS Providers, security and system management staffs, project staffs, host nations, and procurement authorities.

This directive brings together the processes and activities required to bring new systems, solutions and commercial security products into use within NATO.

3. Introducing Secure Systems and Solutions Using Commercial off the Shelf Products into NATO

Figure 1 represents the overall process for introducing secure systems into NATO. It is composed of five major sub-processes:

1. Requirement Capture Process
2. Risk Assessment Process
3. Product Certification and Approval Process
4. Procurement Process
5. Security Accreditation Process

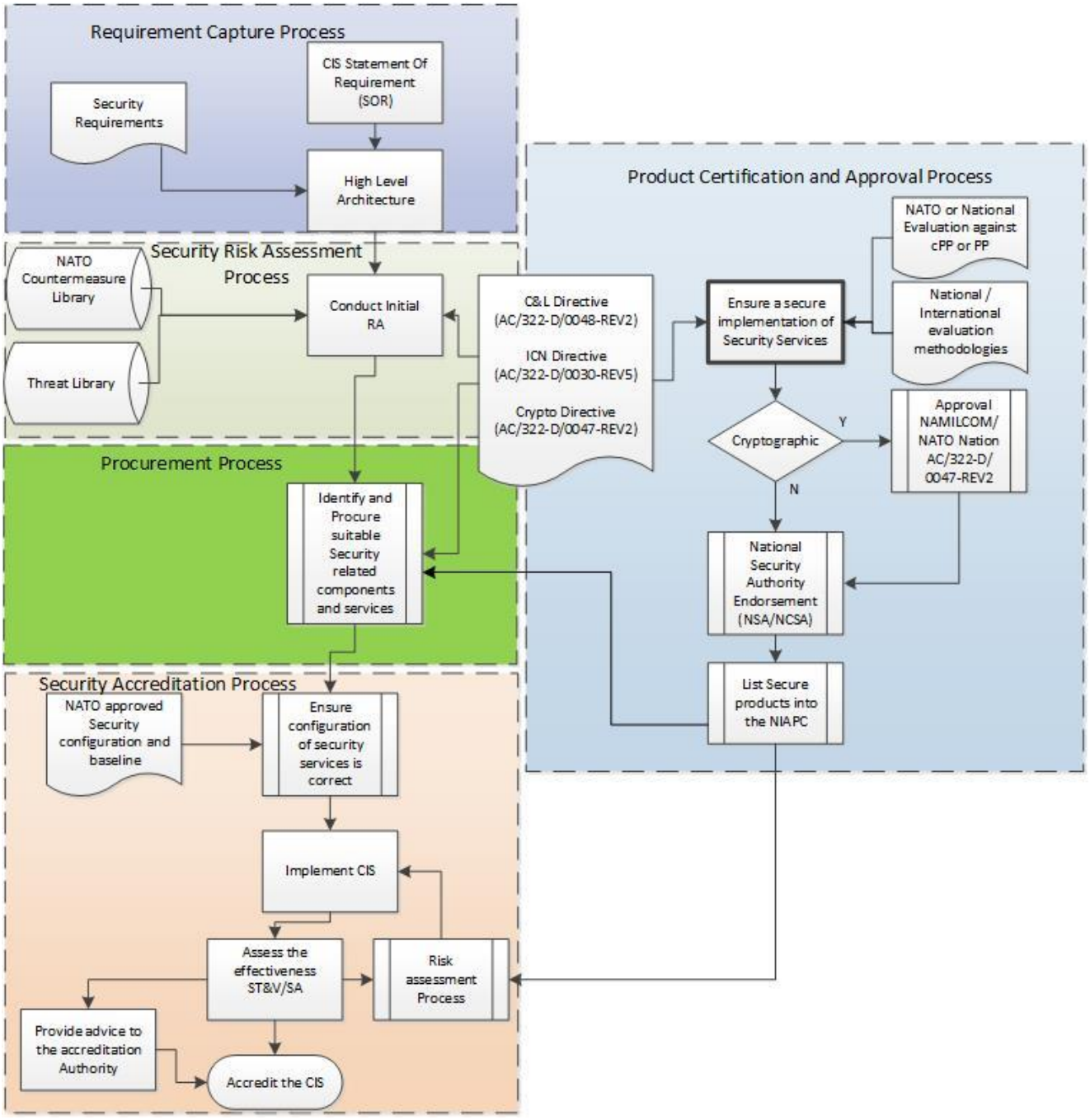

Figure 1 – Overview of the process of introducing secure systems into NATO

The key elements are described below with the entity having primary responsibility indicated in *italics* between parentheses.

3.1. Requirement Capture Process *(Primarily Host Nation[2] of the system)*

The Requirement Capture Process shall take place to identify the technical requirements for a new system following the information exchange requirements presented. One output of the requirement capture process (whether incorporated into the process itself or performed afterwards) shall be a system architecture. The initial security requirements shall be captured and included in this architecture, which must also be subsequently updated to reflect any needs identified by the Risk Assessment Process.

3.2. Risk Assessment Process *(Primarily Host Nation in conjunction with the Security Accreditation Authority of the system)*

The architecture created in the Requirement Capture Process is used to initiate the Risk Assessment Process. This process takes input from the NATO threat and countermeasure libraries as well as the pertinent NATO security policy. The output of the Risk Assessment Process is the Risk Assessment Report. This report identifies the countermeasures to be implemented on the system and any consequential updates to the architecture (in practice both steps are likely to occur in a cycle until a stable, comprehensive, architecture results). The output of the Risk Assessment Process shall also include requirements for supply chain security for security enforcing products (Reference N).

3.3. Product Certification and Approval Process *(Primarily NATO Nations)*

Parts of the Product Certification and Approval Process are likely to take place independently (e.g. through Common Criteria[3] certification). The expected output of the Product Certification or Approval Process is that a NATO nation confirms that the claimed security functionality (e.g. cPP or security target) are effectively implemented in the product to be certified for NATO use. Depending on the information to be handled by the system the security Risk Assessment Process will identify security functional or assurance requirements that shall be fulfilled by products to be certified.

The verification of this requirement can be accomplished by different means. The following means are considered to be equivalent for the verification:

[2] Host Nation refers to the nation, Strategic Command (SC) or agency designated to provide the capability associated with a particular project.
[3] In this document whenever Common Criteria is mentioned this refers to the ISO/IEC 15408 and ISO/IEC 18045 standards.

1. Common Criteria (CC) certification of a product against a NATO approved collaborative Protection Profile (cPP)/Protection Profile (PP) and direct endorsement of a NATO nation.

2. CC certification of a product by a NATO nation complementing the CC certificate with a rationale that the evaluated security functional and assurance requirements are met in accordance with the NATO policy requirements for the product type.

3. Certification or approval of a product by a NATO nation with national/international evaluation methodologies complementing the certificate or approval with a rationale that NATO policy requirements are met.

3.4. Procurement *(Primarily Host Nation of the system)*

This directive does not address the procurement process. This will be determined in the execution of the project. However, attention is drawn to the latest versions of the related directives:

1. NSIP Manual,

2. AC/322-D(2006)0041 Directive on the Selection and Procurement of NATO Common-Funded Cryptographic Systems, Products and Mechanisms,

3. AC/322-D(2004)0030 - INFOSEC Technical and Implementation Directive on the requirement for, and the selection, approval and implementation of Security Tools (ST),

4. AC/322-D(2017)0016 (INV) – Technical & Implementation Directive on NATO Supply Chain Security Requirements for Communication and Information Systems Security Enforcing Products.

When introducing products into NATO CIS, NATO's emission security requirements and related publications must be met.

3.5. Security Accreditation Process *(Primarily Host Nation and Security Accreditation Authority of the system)*

The iterative Security Accreditation Process uses the output from the Security Risk Assessment and Product Certification Processes to identify the appropriate devices for the inclusion into the system. The Security Accreditation Process as a whole is described in the Primary Directive on CIS Security (Reference E), the Management Directive on CIS Security (Reference F) and supporting Guidelines[4].

[4] AC/35-D/1017-REV3 Guidelines for Security Risk Management (SRM) of CIS, and AC/35-D/1021-REV3 Guidelines for the Security Accreditation of CIS.

Once the security enforcing products (which meet the security requirements identified in the Risk Assessment Process) have been selected, a Security Accreditation Authority approved configuration shall be applied.

The CIS can then be implemented and the Security Test and Verification (ST&V) and the Security Audit (SA) can take place. The ST&V shall use the output from the Risk Assessment Process, as documented within the Security Requirement Statement (SRS), to create a test plan confirming the correct implementation of the security enforcing products meeting the security requirements as defined by the Risk Assessment Process. The output of the ST&V and/or SA, including corrective actions reports are provided to the system security. This will allow for the accreditors to make an appropriate accreditation decision.

The deliverable from the overall process shall be security accredited systems built on certified or approved components in their associated configuration. This shall be a repeatable and auditable sequence of events forming a transparent process.

Appendix A - NATO USE OF THE COMMON CRITERIA

1. Purpose

This Appendix sets out the principles of the use of Common Criteria in NATO.

2. Background

This part of the directive discusses the use within NATO of products certified as being evaluated against CC and identifies the process and procedures for their potential use. The use within NATO of CC certified products with suitable security functionality is strongly encouraged.

For the purpose of this directive, the use of certificates recognized under the Common Criteria Recognition Arrangement (CCRA) is recommended. In addition, the use of certificates produced by a national authority of a NATO nation is encouraged. However, on a case-by-case basis, with C3 Board approval, it could also be a partner nation certificate, which is recognized under the CCRA.

3. Related Policies

The NATO Information Management Policy (NIMP) (Reference A) mandates that NATO information, classified and non-classified, shall be protected in accordance with NATO policies (References B and D) and other policies, directives, procedures, and guidance documentation. This is to ensure confidentiality, integrity, availability, authentication and non-repudiation of NATO information throughout its lifecycle, regardless of the medium and format in which the information is held. In addition, the integrity and availability of supporting services and resources shall be ensured.

The Primary Directive on CIS Security provides the connection between NATO policies and the specific CIS Security Technical and Implementation Directives and Guidance. It establishes the security activities in the life-cycle of CIS and other electronic systems and their relationship to supporting CIS directives and guidance.

Common Criteria addresses protection of information from unauthorized disclosure, modification, or loss of use and permits comparability between the results of independent security evaluations. It presents requirements for the Information Technology (IT) security of a product or system under the distinct categories of functional requirements and assurance requirements. The functional requirements define the desired security behaviour whilst assurance requirements are the basis for gaining confidence that the claimed security measures are effective and implemented correctly.

4. CC Applicability Area

Although the CC does not contain security evaluation criteria pertaining to administrative security measures not related directly to the CIS security measures, a significant part of the overall security of a Target of Evaluation (TOE) shall often be achieved through administrative measures such as organizational, personnel, physical, and procedural controls. These measures are identified in the Security Risk Assessment process, implemented in the project/system and tested as a part of the Security Test and Verification (ST&V) as well as the Security Audit in the Security Accreditation Process. Administrative security measures in the operating environment of the TOE are therefore treated as secure usage assumptions where these have an impact on the ability of the CIS security measures to counter the identified threats.

Against the above background, and in accordance with the process described within Section 3.3 in the main body of this Directive:

a. The eligibility of already approved collaborative Protection Profiles (cPP)/Protection Profiles (cPPs/PPs) and supporting documents for a system shall be determined by the CISPIA / CISP in conjunction with the relevant SAA.

b. Where one nation or NATO entity proposes one cPP/PP and requirements, which exceed the cPP/PP, are found, the requirements shall be identified and products accepted against the cPP/PP shall also be assured regarding these additional requirements. Since the additional evaluation activities involved are likely to be performed separately from the certification process (and outside of CCRA), but are likely to be of interest to the developers involved in the International Technical Community (iTC) writing the cPP/PP, releasable requirements shall be reported to the iTC (via NATO members taking part, or through published iTC contact points) to assess suitability for future inclusion in the cPP/PP.

c. Once a cPP/PP and supporting documents have been approved for NATO use, the mapping against the security functionality shall be identified (this is likely to involve publication of a form of “endorsement statement” as used by nations within CCRA, identifying acceptable subsets and combinations of functions. In the case of any additional evaluation activities being required specifically for NATO and falling outside of mutual recognition under CCRA, these shall also be listed).

d. Any subsequent update of a cPP/PP needs to be assessed in a fashion similar to the eligibility determination. If the update of the cPP/PP does have an effect on the security requirements covered by the cPP/PP then this shall be reflected in the mapping of the cPP/PP against the security requirements.

e. When an updated cPP/PP is approved for NATO use, then the CIS security enforcing products to be procured shall follow this updated cPP/PP. The update

of already deployed CIS security enforcing products following this updated cPP/PP will be done through the security accreditation process.

f. Supporting documents are a reusable set of either functional or assurance components combined to satisfy a set of identified security objectives. If already available cPPs or PPs are used, the NATO entity specifying the system security requirements in co-operation with the sponsoring NATO Nation's NCSA or appropriate national security authority shall decide whether the cPPs, PPs and supporting documents (or defined subsets via endorsement statements) are deemed eligible for NATO purposes.

g. cPPs, PPs and supporting documents are already available from NATO nations, non-NATO nations and the commercial sector, this means that NATO does not need to develop every cPP, PP and supporting documents it might require, especially those specifying general security functionality. However, NATO may need to express specific requirements (functions or assurances) as an addition to available cPPs, PPs and supporting documents. It is desired that either NATO or NATO nations participate in the iTC making sure that the NATO requirements are included in the development and updates of cPPs, PPs and supporting documents. If no NATO nation is taking part then consideration should be given to establish an official communication channel (so- called liaison officer) between iTCs and NATO.

5. CPP/PP Approval Process

The cPPs and PPs to be used by NATO will require an approval for use due to the fact that there is a potential for more than one cPP or PP to exist for the same category of equipment.

The following are NATO generic requirements for a cPP or PP:

a. 1. A cPP or PP Supporting Documents considered for NATO use shall be approved by the CCRA prior to NATO approval.

b. When a cPP or PP is used for certifying equipment for NATO use, the product certification shall take place in a NATO nation under the control of a competent national authority.

6. Process of approval of a cPP or PP for NATO use:

a. A cPP or PP and its Supporting Documents is endorsed for NATO use by a NATO nation, this constitutes approval for NATO use of the cPP or PP and its supporting documents.

b. The endorsing nation shall inform the NHQC3S of the endorsement. The endorsing nation shall provide documentary evidence of the cPP or PP and its

supporting documents meeting the NATO CIS security requirements together with the endorsement statement.

c. Evidence shall be made available to all NATO nations and NATO entities upon request. Evidence can be made available to partner nations on a case-by-case basis with C3 Board approval and endorsing nation release authority.

d. The cPP or PP is published for NATO use.

e. If NATO nations identify relevant NATO CIS security requirements which are not met by or are not appropriate in the cPP or PP and its supporting documents then the endorsing nation shall be engaged. If required the C3B or its sub-structure shall be engaged.

7. Use of Other National/International Evaluation Methodologies

The CC evaluation methodology (or national or international equivalent) shall, where appropriate, be used. Alternatively, nations may propose products for use that have been evaluated under different evaluation schemes than the CC.

Where a national or international equivalent is applicable, the appropriate National Security Authority (or appropriate delegated National technical authority) shall make a statement with respect to the conformance of the evaluation to the relevant NATO policies and supporting Directives (References A-K), specifying that the evaluation processes have been carried out in a duly professional manner:

a. on the basis of a national/international CIS Security evaluation criteria and methods;

b. in the context of an Evaluation and Certification/Validation Scheme managed by an official certification body in the proposing country;

If using CC certified products not evaluated under a PP or cPP, it is always necessary to consider the security functionality defined within the Security Target as well as the assurance level/package to confirm that the evaluation performed covers the CIS security requirements.

8. Use of Common Criteria Certification within the Procurement Process

The use of common criteria certification (through CCRA) in the procurement process will be achieved by requiring that the necessary security functionality and assurance requirements are included by the cPPs and PPs and their supporting documents or national equivalents deemed suitable for the CIS security enforcing product concerned. The certification requirements of the CIS security enforcing product are met in the certification process prior to its approval for NATO use.

Appendix B - NATO INFORMATION ASSURANCE PRODUCT CATALOGUE (NIAPC)

1. Purpose

This Appendix sets out the processes and procedures for the establishment, update and maintenance of the NATO Information Assurance Product Catalogue (NIAPC).

2. Scope

This Appendix describes, in detail, the information needed to meet the requirements of the directive and its other appendices[1] and how this can be provided both efficiently, and effectively, by means of a catalogue and associated maintenance mechanisms.

Note, however, that organisational/operational or classification needs may dictate that separate catalogues or parts are used to provide the complete information. Furthermore, the term 'product' is used here in its widest sense since security enforcing functionality may be part of a service (e.g. a cloud service) or a combination of physical/software products and an associated service (e.g. product updates). The key requirement for inclusion in the catalogue are that the product provides security enforcement functions that meet and/or are compatible with relevant NATO policies.

The aim is that the catalogue provides a single point of reference for the initial selection of security enforcing products. Its effectiveness is further extended by the inclusion of lists of common specifications, in the form of protection profiles, as used in Common Criteria certification (both Protection Profiles (PPs) and collaborative protection profiles (cPPs) together with their associated supporting documents as described in Appendix A of this Directive).

The catalogue may also contain national requirements (such as national specifications, national Requirement Profiles for Product Types, etc.) by an NCSA, provided these are relevant for the evaluation and approval of a product, hereinafter referred to as "Requirement Profiles". These Requirement Profiles do not necessarily need to be CC compliant, but according to an assessment of the responsible NCSA, they should be essential and eligible for a listing in the NIAPC together with an approved product.

Since emission security and cryptographic security can form all or parts of the security features of a product, certified TEMPEST vendors, and approved Cryptographic Products and Mechanisms, are also listed in the catalogue.

This Appendix is mandatory and binding to NATO, and NATO nations submitting items for inclusion in the NIAPC.

[1] Particularly Appendix A concerning the use of Common Criteria.

3. Roles and Responsibilities

The NIAPC Provider is responsible for the day-to-day maintenance of the NIAPC and associated entries.

NATO nations (National Communication and Information Systems (CIS) Security Agencies (NCSA), National Tempest Authorities (NTA)) with approved or endorsed Security Enforcing Products, Cryptographic products, TEMPEST product vendors, and cPP/PPs are strongly encouraged to provide the required information to the NIAPC Provider for inclusion into the NIAPC.

Vendor is a company that would like to have their product(s) approved for inclusion in the NIAPC. Their role in this context is purely supportive, easing the administrative burden on the NCSAs, providing requested information and clarification on their products as needed.

NATO Entities identifying security enforcing or cryptographic products found to meet the NATO security requirements are encouraged to provide the required information to the NIAPC Provider for inclusion into the NIAPC.

NATO Staff are responsible for the internal NATO processes for approval of cryptographic products in accordance with Reference H[2], the process for the PP or cPP approval and also the liaison with the NIAPC provider on pre-expiration warnings.

Detailed roles and responsibilities for all relevant NIAPC processes are provided in Section 6 below.

4. Background

Relevant NATO policies, supporting technical directives and guidance documentation call for the implementation of security measures and use of security products in communication, information, other electronic systems, and supporting system services and resources, against loss of confidentiality, integrity or availability.

The NATO CIS Enterprise Security Architecture is based on defined Security Mechanisms.

The security of NATO networks is based on a risk management approach. A Security Risk Assessment (SRA) produces a list of security requirements for the CIS in question. These security countermeasures are grouped within Security Mechanisms for easy traceability throughout the project lifecycle: from the business requirements, architecture/design and implementation, until implementation, test & verification, including continual improvement or decommissioning.

The NIAPC provides the linkage between the Security Mechanisms and the products used to meet the CIS's security requirements. This linkage is implemented through the mapping of Security Mechanisms from the SRA to equipment categories in the NIAPC. This provides the possibility to trace the implementation of a required Security Mechanism as documented in a

[2] Reference H is AC/322-D/0047-REV2 (INV) INFOSEC Technical & Implementation Directive on Cryptographic Security and Cryptographic Mechanisms, 11 March 2009.

SRA through the selection of Security Enforcing, Cryptographic and TEMPEST products and security configuration of these products.

Mapping and traceability fosters the delivery of secure enterprise services and standardization of Security Enforcing, Cryptographic and TEMPEST products to the extent possible whilst remaining business-driven and risk-based.

Project staffs involved in systems/equipment planning, architecture and design, selection procurement and accreditation benefit from having access to information on the current and future availability of information assurance products in order to deliver a risk-based architecture that would also highlight the residual risks, and realistically define how information assurance aspects can be met in systems handling NATO information. Therefore, a current list of NATO Security Enforcing and Cryptographic Products (when available together with product relevant national Requirements Profiles for Product Types), TEMPEST Vendors and cPP/PPs shall be formulated, updated and maintained.

5. NIAPC Operation and Maintenance

The establishment, maintenance, and operation of the NIAPC shall be pursuant to this appendix.

Items submitted for inclusion in the NIAPC shall be endorsed by NCSA or NATO authority based on criteria and standards as specified in NATO policy. Items listed in the NIAPC shall be compliant with relevant NATO policies, directives, and guidance for CIS security.

NATO nations with potentially suitable Security Enforcing and Cryptographic Products (when available together with product relevant national Requirements Profiles for Product Types), TEMPEST Vendors and PPs/cPPs for listing in the NIAPC are strongly encouraged to sponsor inclusion in NIAPC.

NIAPC entries shall be updated at least annually. The sponsors of the submissions to the NIAPC are responsible for ensuring that updated information on the item is provided and that the certificate/approval validity period is stated.

The following caveats shall be included on the NATO Information Assurance Product Catalogue (NIAPC):

- "Users of the NIAPC must understand that choosing a system or product from the list of Security Enforcing and Cryptographic products as well as TEMPEST Vendors and PPs/cPPs does not guarantee an overall secure system/network. There is no guarantee that such systems or products will have compatibility or interoperability".

- "A comprehensive approach is recommended, aggregating all the secure systems/IA products within a security architecture, as established in the Primary Directive on CIS Security (Reference E[3]), and addressing security requirements in a holistic manner."

[3] AC/35-D/2004-REV3, Primary Directive on CIS Security, 15 November 2013.

6. NIAPC Processes

Overview

There are four types of catalogue items discussed here:

- Cryptographic Products[4]
- TEMPEST Vendors
- Security Enforcing Products
- Protection Profiles

The process flows for each are shown in figures 1 to 4 below. In each case the diagram shows the responsibilities of the different actors involved and the decisions and actions needed. The diagrams use conventional flowchart elements (for decision boxes etc.) but also include a specific relationship termed 'Clarification Exchange', described below, in order to avoid the inclusion of rarely used detail that would otherwise clutter the diagram.

Clarification Exchanges

Clarification exchanges arise where some additional information is needed before a decision can be made. The single line on the diagram represents a two way exchange between the NIAPC provider and the relevant other party (possibly multiple exchanges if required). A satisfactory exchange will lead to the conclusion of the decision that initiated the exchange. In the exceptional circumstance that the necessary information/reassurance is not provided, the complete listing process cannot succeed, and would therefore terminate.

Validity dates and monitoring

Although details may differ slightly between the four types of catalogue entries, all processes contain activities that ensure that entries remain valid or are archived. Validity dates and their monitoring by the NIAPC provider are an essential part of this. In some cases (e.g. certified products/Protection Profiles) validity may also depend upon external certification status (e.g. via a certification framework such as the Common Criteria Recognition Arrangement).

Classification

Submitters of information to the NIAPC shall define the classification of all information provided. The NIAPC shall be classified in accordance with the requirements of NATO policies and supporting directives.

[4] For cryptographic products, and Security Enforcing Products, if seen as essential and eligible by the approving NCSA, national Requirements or Requirements Profiles will be provided together with endorsed products to be listed in the NIAPC.

6.1. Cryptographic Products Process

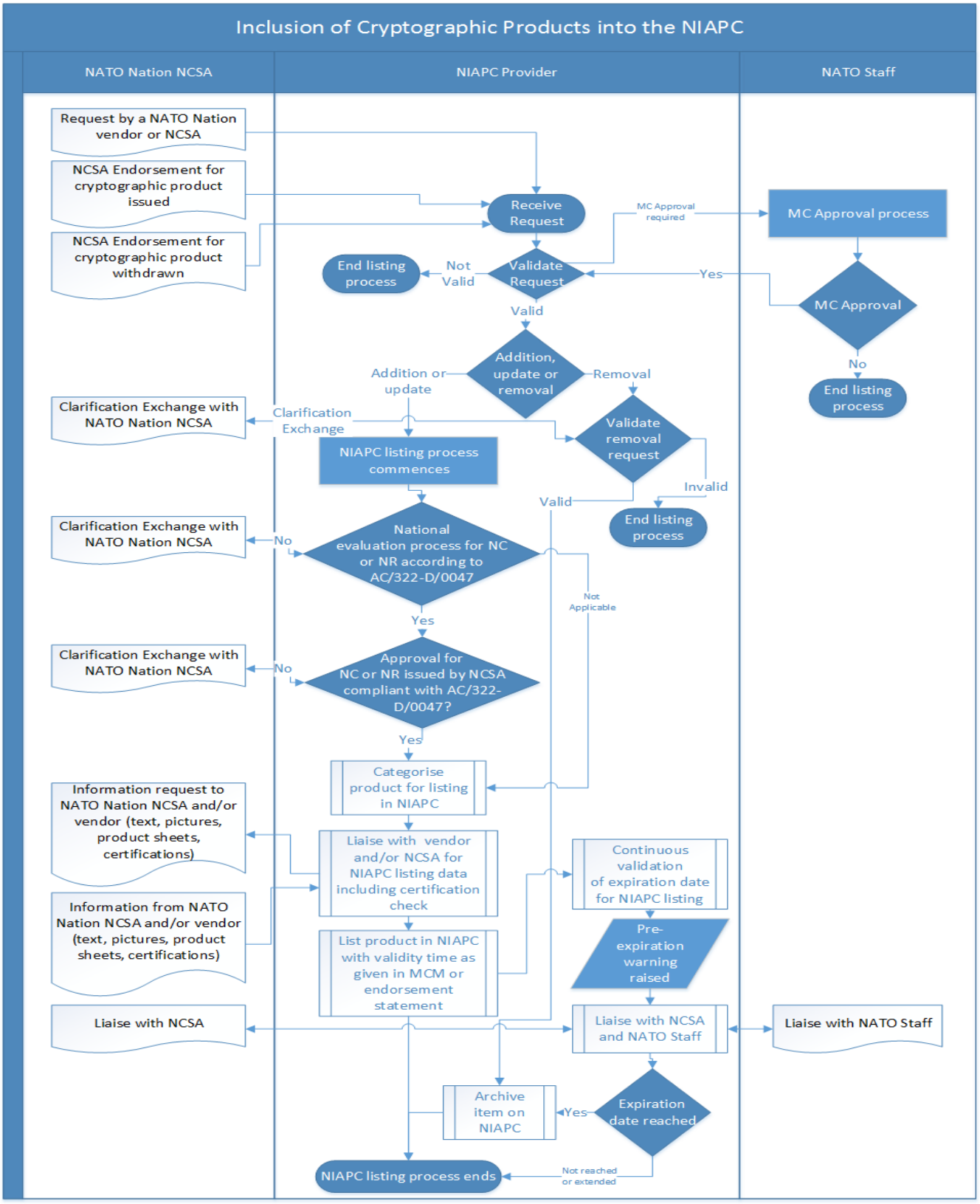

Figure 1 NIAPC Cryptographic Product Process

Figure 1 provides an overview of the process for cryptographic products[5]. The diagram shows the additional step needed for such products where MC approval is involved (see Reference H[6]) together with any clarification exchanges needed for general and cryptographic aspects of the product.

Roles and Responsibilities

NATO Nation Vendor [7]

- Request products for inclusion or update in the NIAPC
- Request products for withdrawal from the NIAPC
- Provide information as required
- Support clarification exchanges as required
- Keep information up to date by review (at least annually with endorsement by NCSA)

NATO Nations (via NCSA)

- Endorse products for inclusion in the NIAPC
- Provide Requirements or Requirements Profiles, if seen essential and eligible for a listing in the NIAPC together with endorsed products.
- Withdraw endorsements where necessary
- Provide information as required
- Support clarification exchanges as required
- Keep information up to date by review (at least annually)
- Take part in pre-expiry discussions as required

NIAPC Provider

- Operate process as in Figure 1
- Receive and validate addition, update and removal requests from NATO Nation vendor or NCSA
- Liaise with NATO staff when Military Committee (MC) approval is needed
- Liaise with NCSA and vendor on information on text, pictures, product sheets and certifications for listings in the NIAPC.
- Liaise with NCSA on clarification exchanges as needed for the different processes
- Liaise with NCSA and NATO Staff on pre-expiration notifications

NATO Staff

- Operate MC Approval/Withdrawal process where required
- Liaise with NIAPC provider regarding pre-expiration warnings

[5] Requiring compliance with AC/322-D/0047-REV2 (INV) INFOSEC Technical & Implementation Directive on Cryptographic Security and Cryptographic Mechanisms, 11 March 2009.

[6] Reference H is AC/322-D/0047-REV2 (INV) INFOSEC Technical & Implementation Directive on Cryptographic Security and Cryptographic Mechanisms, 11 March 2009.

[7] The Vendor role is included for ease of administrative processes. NCSA approval is necessary regardless, therefore a product that does not have national approval will need to obtain it first, and will not be added to the catalogue until national approval is achieved.

6.2. TEMPEST Vendor Process

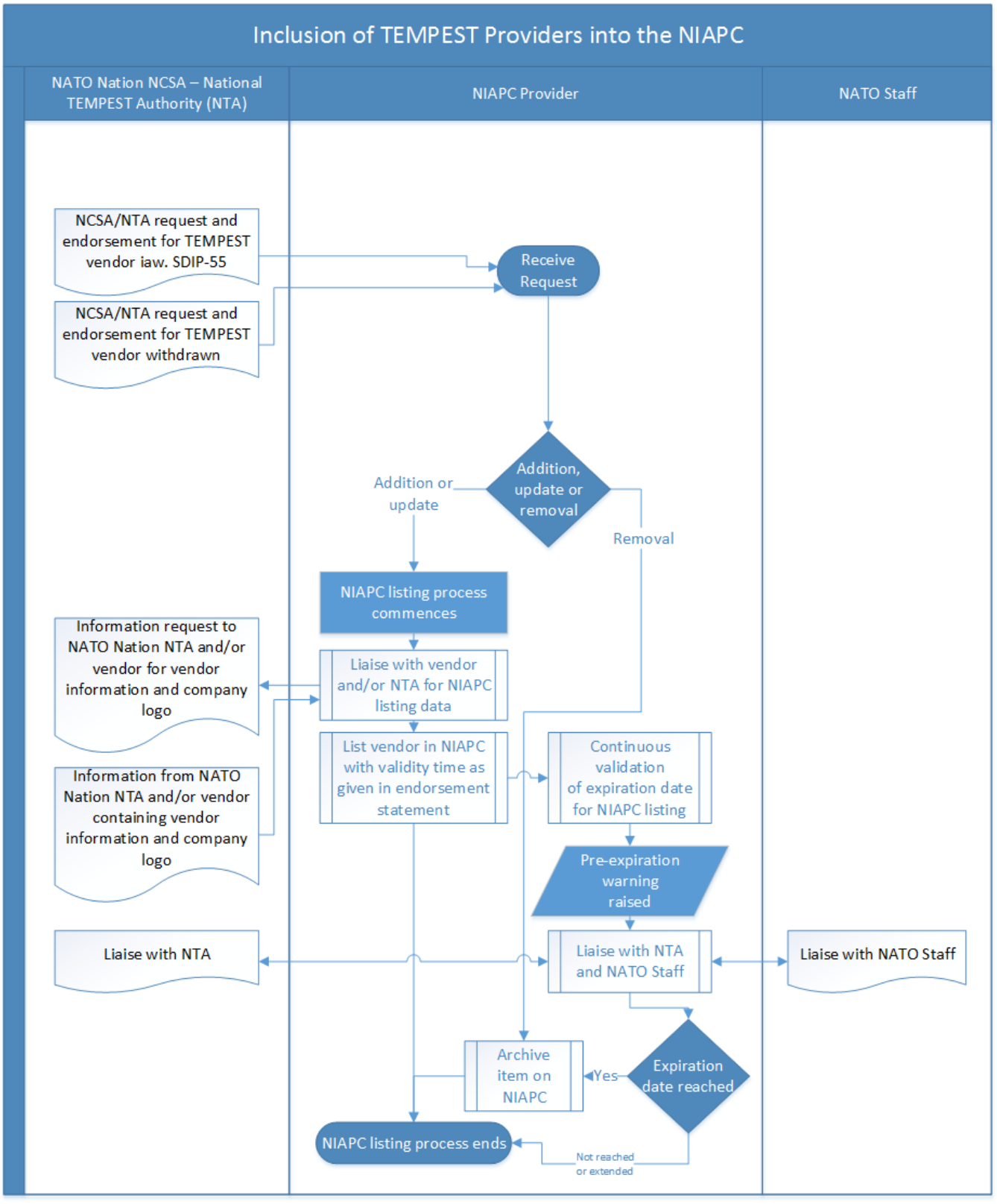

Figure 2 NIAPC TEMPEST Vendor Process

The catalogue items involved in this process are vendors of TEMPEST products (rather than the products themselves) (for background see References O and P[8]) but the underlying process for introduction and removal/archiving of an item remains the same.

Roles and Responsibilities

NATO Nations (via NCSA/NTA)

- Endorse vendors for inclusion in the NIAPC
- Withdraw endorsements where necessary
- Provide information as required
- Support clarification exchanges as required
- Keep information up to date by review (at least annually)
- Take part in pre-expiry discussions as required

NIAPC Provider

- Operate process as in Figure 2
- Receive and validate addition, update and removal requests from NATO Nation NCSA and or NTA
- Liaise with NCSA/NTA and vendor on information on text, pictures, product sheets and certifications for listings in the NIAPC
- Liaise with NCSA/NTA on clarification exchanges as needed for the different processes
- Liaise with NCSA/NTA and NATO Staff on pre-expiration notifications

NATO Staff

- Liaise with NIAPC provider regarding pre-expiration warnings

[8] SDIP-27/2 NATO TEMPEST Requirements and Evaluation Procedures, 4 May 2016 and SDIP-55 NATO TEMPEST Vendor Qualification and Control, 2 September 2010.

6.3. Security Enforcing Product Process

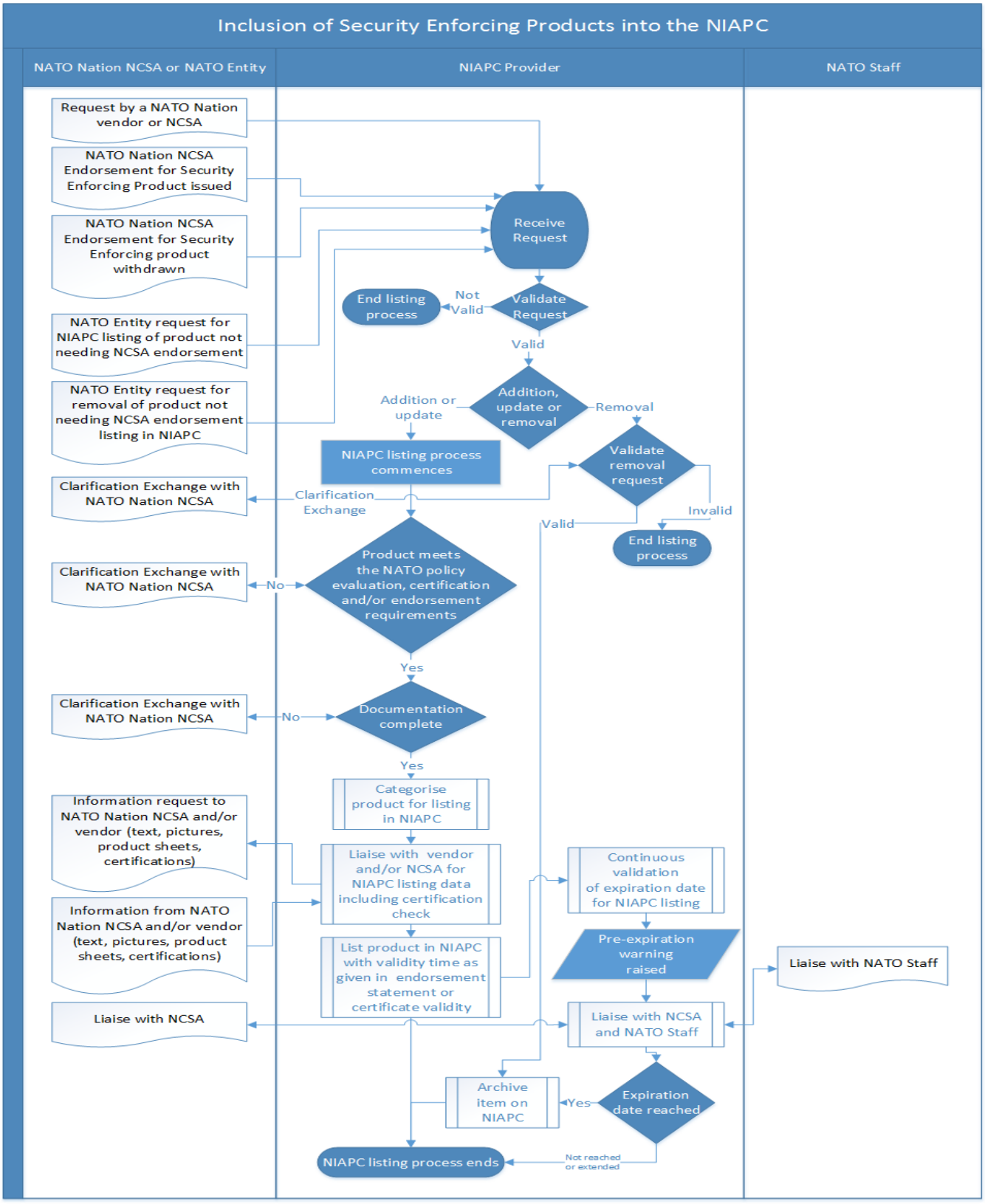

Figure 3 NIAPC Security Enforcing Product Process

Whilst broadly similar to the other process flow diagrams, this diagram incorporates the possibility that NATO entities as well as NATO Nation vendors and NCSAs may request listing/removal of Security Enforcing Products[9]. The continuous validation activity also takes account of the underlying product certification status (e.g. under a certification framework such as the Common Criteria Recognition Arrangement). Other requirements are:

- Products listed in the NIAPC shall be in receipt of a NATO, national or international approval or certification. In instances where this is other than Common Criteria recognition Arrangement based then the product must be in receipt of a finalised national evaluation and approval by a NATO Nation NCSA.
- This input should include Security Target and security objectives, together with recommendations and environmental hypotheses, and shall include all approved or certified product descriptions, technical security feature explanations, national approval or certification report, user guidance and approved or certified configuration guide. If specifications or Requirement Profiles are mandatory and relevant for a national approval, these documents shall be provided by the NCSA.
- Where other national or international evaluation methodologies are used, the appropriate NCSA shall provide, as part of the submission, a rationale showing how the evaluated security functional and assurance requirements are met in accordance with the NATO policy requirements for the product type.
- Only Security Enforcing Products sponsored by a NATO nation, and considered suitable for use by that nation for protection of both national and NATO information, shall be listed in the NIAPC. Cryptographic mechanisms forming part of any such product shall conform to Reference H[10].
- Products sponsored by a NATO nation can also include those developed and produced outside of a NATO nation.
- All Security Enforcing Products listed in the NIAPC must be commercially available.

Roles and Responsibilities

NATO Nation Vendor

- Request products for inclusion or update in the NIAPC
- Request products for withdrawal from the NIAPC
- Provide information as required
- Support clarification exchanges as required
- Keep information up to date by review (at least annually with endorsement by NCSA)

NATO Nations (via NCSA) or NATO Entity

- Endorse Security Enforcing Products for inclusion in the NIAPC
- Provide Requirements or Requirements Profiles, if seen essential and eligible for a listing in the NIAPC together with endorsed products.
- Update information as required (via the same mechanism)

[9] NOTE: In the case of a removal, this will always involve the originator of the listing.

[10] AC/322-D/0047-REV2 (INV), INFOSEC Technical & Implementation Directive on Cryptographic Security and Cryptographic Mechanisms, 11 March 2009.

- Withdraw endorsements where necessary
- Provide information as required
- Support clarification exchanges as required
- Keep information up to date by review (at least annually)
- Take part in pre-expiry discussions as required

NIAPC Provider

- Operate process as in Figure 3
- Receive and validate addition, update and removal requests from NATO Nation vendor or NCSA or NATO Entity
- Liaise with NCSA, NATO Entity and vendor on information on text, pictures, product sheets and certifications for listings in the NIAPC.
- Liaise with NCSA on clarification exchanges as needed for the different processes
- Liaise with NCSA and NATO Staff on pre-expiration notifications

NATO Staff

- Liaise with NIAPC provider regarding pre-expiration warnings

6.4. Protection Profile Process

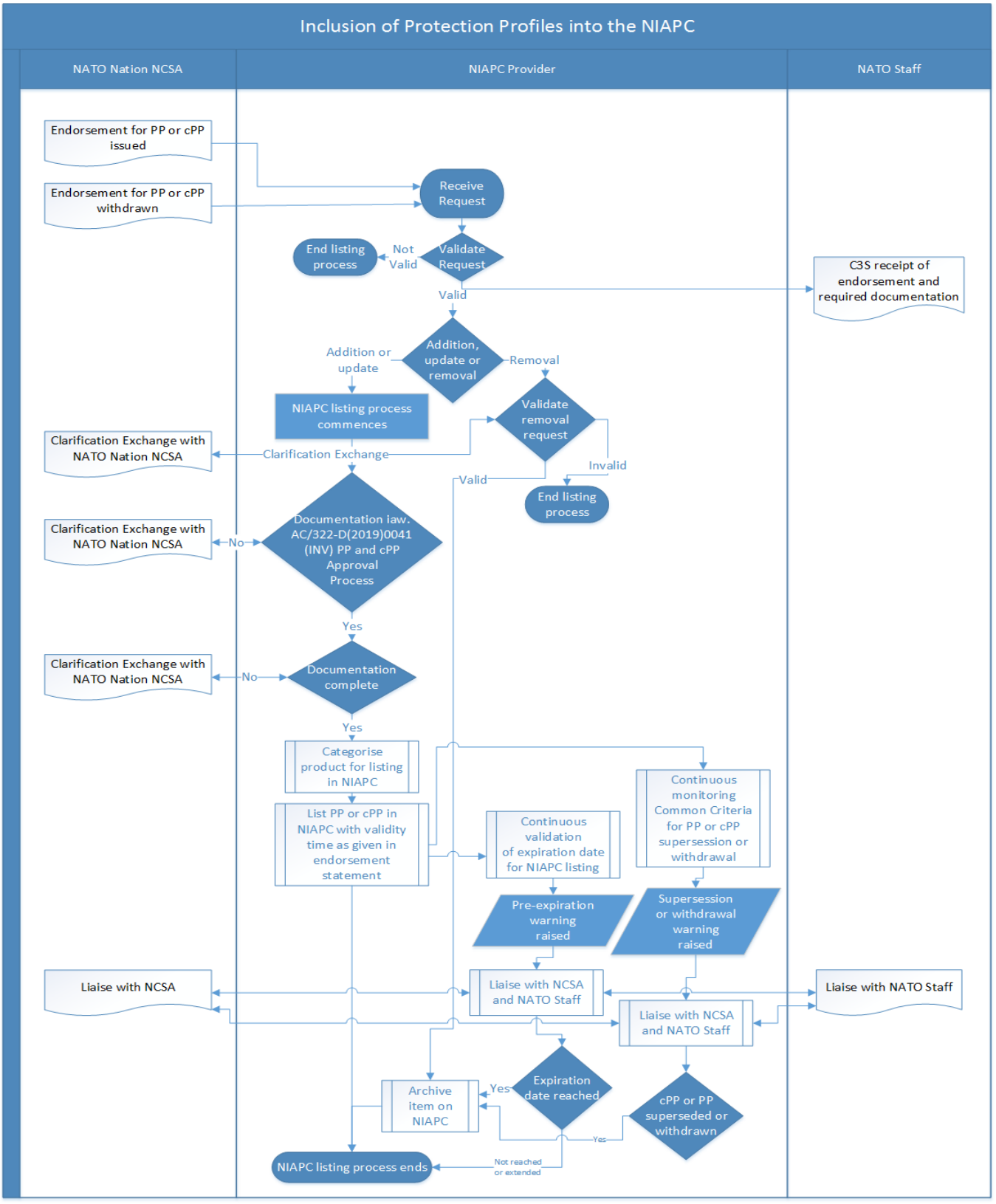

Figure 4 NIAPC Protection Profiles Process

Protection Profiles (PP) can be used to define the requirements, in an efficient, common manner, for products from multiple vendors (e.g. covering NATO requirements for firewalls). In fast moving technologies[11] the PP, and its associated supporting documents are likely to be frequently updated. It is therefore necessary to ensure the appropriate levels of awareness and engagement are provided for NATO staff. While the general process is broadly the same as that used for products, in this process, C3S are informed of the initial endorsement (together with required documentation), and the monitoring process, used after listing has occurred, reflects the fact that the PP development process is dynamic, and takes account of both the original endorsement validity date, and the wider validity/superseding of the profiles and supporting documents within a certification framework such as the Common Criteria Recognition Arrangement (since these dates may be earlier).

The list of cPP/PPs shall be updated and maintained, based on input provided, and applying the rules and requirements given in Appendix A “NATO Use of Common Criteria”.

Roles and Responsibilities

NATO Nations (via NCSA) or NATO Entity

- Endorse cPPs and PPs for inclusion in the NIAPC
- Withdraw endorsements where necessary
- Provide information as required
- Support clarification exchanges as required
- Keep information up to date by review (at least annually)
- Take part in pre-expiry discussions as required

NIAPC Provider

- Operate process as in Figure 4
- Receive and validate addition, update and removal requests from NATO Nation NCSA
- Deliver received PP or cPP endorsement and required documentation to NATO Staff
- Liaise with NCSA on clarification exchanges as needed for the different processes
- Liaise with NCSA and NATO Staff on pre-expiration notifications

NATO Staff

- Receive and acknowledge documentation from NIAPC provider
- Liaise with NIAPC provider regarding pre-expiration warnings
- Liaise with NIAPC provider regarding external certification changes

[11] Where either the technology or the threat, or both are rapidly evolving.

7. NIAPC Request Templates

For the most common requests the following template letters may be used as a basis when submitting or updating information:

Endorsement of Common Criteria certified product for NATO use

The Common Criteria certified product *<insert suitable references>* has been examined under the NCSA of *<insert NATO Nation>*.

The evaluated security functional and assurance requirements are met in accordance with the NATO policy requirements for the product type.

Documentation on the examination providing the rationale behind the endorsement is available upon request.

The NCSA of *<insert NATO Nation>* endorses the product for NATO use and requests that the product is listed in the NIAPC.

This endorsement is given with a validity until *<insert validity date>* at which time the product shall be archived on the NIAPC.

Endorsement of a nationally evaluated product for NATO use

The product *<insert suitable references>* has been evaluated under the NCSA of *<insert NATO Nation>*.

Optional if deemed necessary by the approving nation: The NCSA of *<insert NATO Nation>* evaluated *<insert product>* according to the *<insert national requirements/requirements profile>* for which the details are provided in an enclosure.

The evaluated security functional and assurance requirements are met in accordance with the NATO policy requirements for the product type.

Documentation on the evaluation providing the rationale behind the endorsement is available upon request.

The NCSA of *<insert NATO Nation>* approves/certifies product *<insert suitable reference(s)>* for use, and recommends the product for NATO use, requesting that the product is listed in the NIAPC.

This endorsement is given with a validity until *<insert validity date>* at which time the product shall be archived on the NIAPC.

Endorsement of collaborative Protection Profile (cPP) / Protection Profile (PP) for NATO use

The Common Criteria cPP/PP *<insert suitable reference(s)>* and its associated supporting documents *<insert suitable reference(s)>* have been examined under the NCSA of *<insert NATO Nation>*.

The evaluated security functional and assurance requirements are met in accordance with the NATO policy requirements for the product type covered by the cPP/PP.

Documentation of the examination, providing the rationale behind the endorsement is available upon request.

The NCSA of <*insert NATO Nation*> endorses the cPP/PP for NATO use (under the conditions listed in the associated endorsement statement <*provide a link to endorsement statement on CCRA Portal, or attach the statement*>) and requests that it is listed in the NIAPC.

This endorsement is given with a validity until <*insert validity date*> at which time, unless renewed, the cPP/PP and associated products shall be archived on the NIAPC.