NATO UNCLASSIFIED

22 September 2010

DOCUMENT
AC/322-D(2010)0042
Silence Procedure ends:
22 Oct 2010 15:00

CONSULTATION, COMMAND AND CONTROL BOARD (C3B)

INFOSEC TECHNICAL AND IMPLEMENTATION DIRECTIVE FOR THE NATO INFORMATION ASSURANCE PRODUCT CATALOGUE (NIAPC)

Note by the Secretary

Reference: AC/322(SC/4)WP(2010)0007

1. The NATO Information Assurance Product Catalogue (NIAPC) established under this Directive (Enclosure 1) provides NATO nations, and NATO civil and military bodies with a catalogue of Information Assurance (IA) products, Protection Profiles and Packages that are in use or available for procurement to meet operational requirements.

2. The Information Assurance Sub-Committee agreed the directive under a Silence Procedure ending 9 September 2010 (Ref.).

3. Unless comments to the contrary are received by the Action Officer **by 15:00 hrs** on **Friday, 22 October 2010**, the Directive will be considered to have been approved by the C3 Board.

(Signed) B. LURQUIN

Enclosure 1: INFOSEC T&I Directive for the NIAPC

1 Enclosure

Action Officer: Cdr Pahlke, 5512
Original: English

ENCLOSURE 1
AC/322-D(2010)0042

NATO

INFOSEC TECHNICAL AND IMPLEMENTATION DIRECTIVE FOR THE NATO INFORMATION ASSURANCE PRODUCT CATALOGUE (NIAPC).

Processes and procedures for the establishment, update and maintenance of the NATO Information Assurance Product Catalogue (NIAPC).

Contents

References:

1. C-M(2007)0118, NATO Information Management Policy (NIMP), 11 December 2007

2. C-M(2002)49. Security within the North Atlantic Treaty Organisation, 17 June 2002 including COR 7 dated 19 August 2009

3. AC/322-D/0052 Rev 1 (AC/35-D/2004 Rev 1). Primary Directive on INFOSEC; 19 October 2006

4. SDIP 27 NATO TEMPEST requirements and Evaluation procedures, November 2005

5. SDIP 55 TEMPEST Product Qualification and Control, August 2009

6. AC/322-D(2004)0030. INFOSEC T & I Directive on the requirement for, and the selection, approval and Implementation of Security Tools; 17 May 2004

7. AC/322-D(2006)0006, INFOSEC T & I Guidance on the Use of the Common Criteria within NATO, 31 January 2006

Purpose

1. This INFOSEC Technical and Implementation Directive is published by the NATOC3 Board in support of the NATO Information Management Policy (NIMP), NATO Security Policies for the protection of classified and non-classified information, and the Primary Directive on INFOSEC. It establishes the process and procedures for the establishment, update and maintenance of the NATO Information Assurance Product Catalogue (NIAPC).

2. The purpose of the NATO Information Assurance Product Catalogue (NIAPC) established under this Directive is to provide NATO nations, and NATO civil and military bodies a catalogue of Information Assurance (IA) products, Protection Profiles and Packages that are in use or available for procurement to meet operational requirements.

Scope

3. This INFOSEC Directive is mandatory and binding upon the IA Branch of the NHQC3S, SECAN, and NATO nations submitting IA products, Protection Profiles, or Packages onto the NATO Information Assurance Product Catalogue (NIAPC). NATO nations submitting IA products, Protection Profiles or Packages on the NATO Information Assurance Product Catalogue (NIAPC) shall provide the required information on these products, Protection Profiles or Packages when requested by the IA Branch of the NHQC3S and shall update that information at regular intervals.

Responsibilities

4. The IA Branch of the NHQC3S is responsible for ensuring the implementation of this directive. The NATO INFOSEC Technical Centre (NITC) is responsible for the day to day management of the NATO Information Assurance Product Catalogue (NIAPC). NATO nations with approved or endorsed IA products, Protection Profiles or Packages are responsible for, and are strongly encouraged to provide the required information on these products, Protection Profiles or Packages to the IA Branch of the NHQC3S and the NIATC for inclusion into the NATO Information Assurance Product Catalogue (NIAPC). National input should be provided at least annually. However, the NIAPC will be constantly updated by NIATC based on input received.

Background

5. NATO Security Policies, supporting directives and guidance documentation call for the implementation of security measures and use of security products to protect information processed, stored or transmitted (handled) in communication, information, other electronic systems, and supporting system services and resources, against loss of confidentiality, integrity or availability.

6. Project staffs involved in systems/equipment planning, selection and procurement need to have access to information on the current and future availability of IA products in order to realistically define how IA aspects can be met in systems handling NATO information. Therefore, a definitive, current list of NATO IA
Products, Protection Profiles and Packages shall be formulated, updated and maintained.

NIAPC Functions

7. The central functions of the NIAPC are, therefore, as follows.

7.1. The creation, maintenance and operation of the NIAPC is pursuant to this directive.

7.2. The NIAPC shall be the primary and preferred route to market for all IA products for use within NATO.

7.3. Products listed in the NIAPC shall be selected on the basis of criteria and standards as established and set by this directive.

7.4. Selection of products for inclusion in the NIAPC shall be such as to enable and support compliance with NATO IA policies.

7.5. Procurement of products listed in the NIAPC shall be enabled using common processes and procedures.

7.6. The NIAPC shall enable inclusion of IA products meeting the NIAPC criteria and standards from all NATO member nations.

7.7. NATO nations with potentially suitable candidates for listing in the NIAPC are strongly encouraged to sponsor inclusion in NIAPC.

NIAPC categories

8. The NATO Information Assurance Product Catalogue (NIAPC) shall contain Manufacturers, Products, Protection Profiles and Packages in the following IA categories:

Cryptographic Products and Cryptographic Mechanisms

8.1 CA (Certificate Authority)
8.2 Communications Encryption
8.3 Disk/File Encryption
8.4 Email Signing & Encryption
8.5 IP Encryption
8.6 Key Management
8.7 PKI (Public Key Infrastructure)
8.8 VPN (Virtual Private Network)
8.9 Other

Emission Security

8.10 Certified TEMPEST Vendors

Information Assurance (IA) Security Products

8.11 Access Control
8.12 Application Control & Configuration
8.13 Asset Management
8.14 Auditing Software
8.15 Authentication
8.16 Operating Systems
8.17 Patch Management
8.18 Physical Security
8.19 Policy Authoring
8.20 Record Management
8.21 Risk Assessment / Decision Support
8.22 Archive & Disaster Recovery
8.23 Smart Cards
8.24 Trouble Ticketing
8.25 WEB Security Suite
8.26 Wireless Security
8.27 Biometrics
8.28 Content Checking / Filtering
8.29 Desktop Security Suite
8.30 Disk Management
8.31 Document Management
8.32 Email Policy Enforcement
8.33 Email Security Suite
8.34 Firewall

8.35 Identity Management
8.36 Information Rights Management (IRM)
8.37 IT Health Check
8.38 Malware Protection
8.39 Network Management
8.40 Network Security Suite
8.41 Disk Erasure
8.42 Computer Forensics
8.43 Intrusion Detection and Prevention

Protection Profiles

Additional categories may be added to meet future IA development.

Cryptographic Products and Cryptographic Mechanisms

9. Only cryptographic products which are developed and produced in a NATO member Nation and which are evaluated and approved in accordance with the INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms, by the developing nations National Communications Security Authority (NCSA) are eligible to be submitted for inclusion to the NATO Information Assurance Product Catalogue (NIAPC). Those products subject to an additional release action shall be so noted in the product's listing.

10. This list of cryptographic products and cryptographic mechanisms should include both those products which are approved for use in NATO and national systems to protect NATO classified information, as well as all products produced by NATO member nations which are evaluated and approved for use by non-NATO nations and International Organizations to protect NATO classified information.

11. The list of cryptographic products and cryptographic mechanisms shall be updated and maintained by the NIATC on behalf of the NHQC3S based on input provided by the National Communications Security Authority of NATO member nations.

Emission Security - Certified TEMPEST company list

15. This list will contain certified TEMPEST companies that are compliant with SDIP 55 and endorsed by the National TEMPEST Authority[1](NTA) of the nation in which they reside. In accordance with SDIP 55 these certified companies are authorized to sell SDIP 27 Level A and SDIP 27 Level B products to NATO. SDIP 55 details the procedures that must be in place within a certified TEMPEST company before their inclusion into the NIAPC.

17. The list of Certified TEMPEST companies shall be updated and maintained by the NIATC based on input provided by the NATO Nation's National TEMPEST Authority.

[1] In most NATO Nations the National TEMPST Authority is within the National Communication Security Authority.

Information Assurance (IA) Security Products

18. The aim of the list of IA Security Products is to provide security approval authorities (for example, Security Accreditation Authorities), CIS Operating Authorities, CIS planners and implementers, project staffs, and users in NATO Member Nations, NATO civil and military bodies a baseline of information with respect to available evaluated and certified/validated IA security products which can be used as guidance for meeting NATO security requirements in CIS.

19. Products listed in the NIAPC shall be in receipt of a recognised NATO, national or international evaluation or certification. In instances where this is other than Common Criteria then the product must be in receipt of a finalized national evaluation and approval by a NATO NCSA. Where a national or international equivalent is applicable, the appropriate National Security Authority shall make, as part of the submission, a statement with respect to the equivalence of the evaluation to the Common Criteria.

20. For Common Criteria evaluated and certified products, only products sponsored within a NATO member nation and considered suitable for use within that nation for protection of national information shall be listed in the NIAPC[2].

21. The following caveat shall be included as a preface to the IA Security products listed on the NATO Information Assurance Product Catalogue (NIAPC):

"Users of the Product, Protection Profile and Package list must understand that choosing a system or product from the list of IT Security products does not guarantee an overall secure system/network. There is no guarantee that such systems or products will have compatibility or interoperability".

22. The List of IA Security Products shall be updated and maintained by the NIATC on behalf of the NHQC3S based on input provided by a NATO National Communication Security Authority or a recognized NATO or National Certification/Validation Authorities (i.e. SECAN, EUSEC). See the Update and Maintenance Section for further details on the update and maintenance of the NATO Information Assurance Product Catalogue (NIAPC).

23. Additional information on Common Criteria validated/certified products that have been included on the NIAPC may be found at the following Web Site: **www.commoncriteriaportal.org**.

[2] Sponsored within a NATO member nation" also includes product developed and produced outside NATO member states, but sponsored by a NATO member state. This situation requires special consideration within the sponsoring nation. Cryptographic mechanisms forming part of any such product shall conform with AC322- D/0047 Rev 2 (INV).

Protection Profiles and Packages

24. A Protection Profile (PP) defines an implementation-independent set of security requirements and objectives for a category of products or systems, which meet similar consumers' needs for IA security. A PP is intended to be reusable and to define requirements that are known to be useful and effective in meeting the identified objectives.

25. A Package is a reusable set of either functional or assurance components (e.g. an Evaluation Assurance Level) combined together to satisfy a set of identified security objectives.

26. Only evaluated and certified/validated Protection Profiles and Packages, which are developed by NATO or NATO member states and/or sponsored by NATO nations, shall be included in the NIAPC.

27. The list of Protection profiles shall be updated and maintained by the NIATC based on input provided by the NATO Nation's National Communication Security Authority

Update and Maintenance of the NATO Information Product Catalogue (NIAPC).

28. The NIAPC shall be maintained by the NIATC. National Security Authorities are encouraged to submit entries or removals from the NIAPC any time to the INFOSEC Branch of the NHQC3S or directly to the NIATC. The National Security Authorities must ensure that the products they sponsor remain fit for purpose and inform NIATC of any security issues with the products.

29. Submitters of information to the NIAPC shall indicate the classification of all information provided. The NIAPC shall be classified in accordance with the requirements of NATO Security Policy and supporting directives.

30. The NIAPC shall be updated and maintained by the NIATC based on input provided by the NATO Nation's National Communication Security Authority or National Security Authority.

31. The NIAPC and associated documentation for inclusion of products in the catalogue can be found at **www.ia.nato.int**