

FINLANDS FÖRFATTNINGSSAMLINGS FÖRDRAGSSERIE

Utgiven i Helsingfors den 22 augusti 2023

56/2023

(Finlands författningssamlings nr 922/2023)

Statsrådets förordning om avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet samt säkerhetsbestämmelserna

I enlighet med statsrådets beslut föreskrivs med stöd av 2 och 3 § i lagen om avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet samt säkerhetsbestämmelserna (907/2023):

1 §

Det i Bryssel den 6 mars 1997 mellan parterna i nordatlantiska fördraget ingångna avtalet om informationssäkerhet samt de säkerhetsbestämmelser som antagits med stöd av avtalet, sådana de lyder ändrade i handlingen C-M(2002)49-REV1 av den 20 november 2020, träder i kraft den 23 augusti 2023 enligt vad som har avtalats.

Avtalet och säkerhetsbestämmelserna har godkänts av riksdagen den 20 juni 2023 och av republikens president den 14 juli 2023. Finlands anslutningsinstrument har deponerats hos Förenta staternas regering den 24 juli 2023.

2 §

De bestämmelser i avtalet och i säkerhetsbestämmelserna som inte hör till området för lagstiftningen ska gälla som förordning.

3 §

Lagen om avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet samt säkerhetsbestämmelserna (907/2023) träder i kraft den 23 augusti 2023.

4 §

Denna förordning träder i kraft den 23 augusti 2023.

Helsingfors den 17 augusti 2023

Utrikeshandels- och utvecklingsminister Ville Tavio

Utrikesråd Päivi Kaukoranta

Avtalstext

AVTAL MELLAN PARTERNA I NORDATLANTISKA FÖRDRAGET OM INFORMATIONSSÄKERHET

AGREEMENT BETWEEN THE PARTIES TO THE NORTH ATLANTIC TREATY FOR THE SECURITY OF INFORMATION

Parterna i nordatlantiska fördraget, undertecknat i Washington den 4 april 1949,

The Parties to the North Atlantic Treaty, signed at Washington on 4th April, 1949.

som bekräftar att effektivt politiskt samråd, effektivt samarbete och effektiv planering i försvarsfrågor i syfte att uppnå målen för fördraget förutsätter utbyte av säkerhets- skyddsklassificerad information mellan parterna,

Reaffirming that effective political consultation, cooperation and planning for defence in achieving the objectives of the Treaty entail the exchange of classified information among the Parties.

som anser att det mellan regeringarna för parterna i nordatlantiska fördraget behövs bestämmelser om ömsesidigt skydd av sådan säkerhetsskyddsklassificerad information som de utbyter sinsemellan,

Considering that provisions between the Governments of the Parties to the North Atlantic Treaty for the mutual protection and safeguarding of the classified information they may interchange are necessary.

som är medvetna om att en allmän ram för säkerhetsstandarder och säkerhetsförfaranden behövs, och

Realising that a general framework for security standards and procedures is required.

som handlar för egen och för Nordatlantiska fördragsorganisationens räkning,

Acting on their own behalf and on behalf of the North Atlantic Treaty Organization,

har kommit överens om följande.

have agreed as follows:

Artikel 1

Article 1

Parterna ska

The Parties shall:

i. säkerställa skyddet av

(i) protect and safeguard:

a. säkerhetsskyddsklassificerad information (se bilaga I) som är märkt som sådan och som härrör från Nordatlantiska fördragsorganisationen (Nato) (se bilaga II) eller som en medlemsstat lämnar till Nato,

(a) classified information (see Annex I), marked as such, which is originated by NATO (see Annex II) or which is submitted to NATO by a member state;

b. säkerhetsskyddsklassificerad information som är märkt som sådan och som en medlemsstat lämnar till en annan medlemsstat till stöd för något av Natos program, projekt eller kontrakt,

(b) classified information, marked as such, of the member states submitted to another member state in support of a NATO programme, project, or contract,

ii. bibehålla säkerhetsskyddsklassificeringen av den information som avses i punkt i och göra sitt yttersta för att skydda informationen i enlighet därmed,

iii. inte använda sådan säkerhetsskyddsklassificerad information som avses i punkt i för andra ändamål än de som fastställs i nordatlantiska fördraget och i de beslut och resolutioner som hänför sig till det fördraget,

iv. inte röja sådan information som avses i punkt i för parter som inte hör till Nato utan samtycke från den som informationen härrör från.

(ii) maintain the security classification of information as defined under (i) above and make every effort to safeguard it accordingly;

(iii) not use classified information as defined under (i) above for purposes other than those laid down in the North Atlantic Treaty and the decisions and resolutions pertaining to that Treaty;

(iv) not disclose such information as defined under (i) above to non-NATO Parties without the consent of the originator.

Artikel 2

I enlighet med artikel 1 i detta avtal ska parterna säkerställa att det inrättas en nationell säkerhetsmyndighet för Natos verksamhet för att genomföra säkerhetsskyddsåtgärder. Parterna ska utarbeta och tillämpa säkerhetsstandarder som säkerställer en gemensam skyddsnivå för säkerhetsskyddsklassificerad information.

Artikel 3

1. Parterna ska säkerställa att alla deras medborgare som i sin tjänsteutövning behöver eller kan komma att få åtkomst till information som säkerhetsskyddsklassificerats som CONFIDENTIAL eller högre har godkänts vid en adekvat säkerhetsprövning innan de inleder tjänsteutövningen.

2. Förfarandena för säkerhetsprövning ska utformas så att det fastställs huruvida en person, med beaktande av personens lojalitet och pålitlighet, kan få åtkomst till säkerhetsskyddsklassificerad information utan att utgöra en oacceptabel säkerhetsrisk.

3. Parterna ska på begäran samarbeta med de andra parterna när det gäller genomförandet av deras respektive förfaranden för säkerhetsprövning.

Article 2

Pursuant to Article 1 of this Agreement, the Parties shall ensure the establishment of a National Security Authority for NATO activities which shall implement protective security measures. The Parties shall establish and implement security standards which shall ensure a common degree of protection for classified information.

Article 3

(1) The Parties shall ensure that all persons of their respective nationality who, in the conduct of their official duties, require or may have access to information classified CONFIDENTIAL and above are appropriately cleared before they take up their duties.

(2) Security clearance procedures shall be designed to determine whether an individual can, taking into account his or her loyalty and trustworthiness, have access to classified information without constituting an unacceptable risk to security.

(3) Upon request, each of the Parties shall cooperate with the other Parties in carrying out their respective security clearance procedures.

Artikel 4

Generalsekretären ska säkerställa att Nato tillämpar de bestämmelser i detta avtal som är tillämpliga på organisationen (se bilaga III).

Artikel 5

Detta avtal hindrar inte på något sätt att parterna ingår andra avtal som gäller utbyte av sådan säkerhetsskyddsklassificerad information som härrör från parterna och som inte påverkar tillämpningsområdet för detta avtal.

Artikel 6

a. Detta avtal ska vara öppet för undertecknande av parterna i nordatlantiska fördraget och ratificeras, godtas eller godkänns. Ratifikations-, godtagande- eller godkännandeinstrumentet ska deponeras hos Amerikas förenta staters regering.

b. Detta avtal träder i kraft 30 dagar efter den dag då två signatärstater har deponerat sina ratifikations-, godtagande- eller godkännandeinstrument. Med avseende på varje annan signatärstat träder avtalet i kraft 30 dagar efter det att respektive stats ratifikations-, godtagande- eller godkännandeinstrument har deponerats.

c. I fråga om de parter för vilka detta avtal har trätt i kraft ersätter detta avtal det säkerhetsavtal mellan parterna i Nordatlantiska fördragsorganisationen som godkändes av Nordatlantiska rådet den 19 april 1952 i bilaga A (punkt 1) till tillägget till bilagan till D.C.2/7 och senare inkluderats i bilaga A (punkt 1) till C-M(55)15(Final), som godkändes av Nordatlantiska rådet den 2 mars 1955.

Artikel 7

Detta avtal ska vara öppet för anslutning av varje ny part i nordatlantiska fördraget i en-

Article 4

The Secretary General shall ensure that the relevant provisions of this Agreement are applied by NATO (see Annex III).

Article 5

The present Agreement in no way prevents the Parties from making other Agreements relating to the exchange of classified information originated by them and not affecting the scope of the present Agreement.

Article 6

(a) This Agreement shall be open for signature by the Parties to the North Atlantic Treaty and shall be subject to ratification, acceptance or approval. The instruments of ratification, acceptance or approval shall be deposited with the Government of the United States of America;

(b) This Agreement shall enter into force thirty days after the date of deposit by two signatory States of their instruments of ratification, acceptance or approval. It shall enter into force for each other signatory State thirty days after the deposit of its instrument of ratification, acceptance or approval;

(c) This Agreement shall with respect to the Parties for which it entered into force supersede the "Security Agreement by the Parties to the North Atlantic Treaty Organization" approved by the North Atlantic Council in Annex A (paragraph 1) to Appendix to Enclosure to D.C.2/7, on 19th April, 1952, and subsequently incorporated in Enclosure "A" (paragraph 1) to C-M(55)15(Final), approved by the North Atlantic Council on 2nd March, 1955.

Article 7

This Agreement shall remain open for accession by any new Party to the North Atlantic Treaty, in accordance with its own

lighet med den partens konstitutionella förfaranden. Partens anslutningsinstrument ska deponeras hos Amerikas förenta staters regering. Med avseende på varje anslutande stat träder avtalet i kraft 30 dagar efter den dag då dess anslutningsinstrument deponeras.

Artikel 8

Amerikas förenta staters regering ska underrätta de övriga parternas regeringar om deponeringen av varje ratifikations-, godtagande-, godkännande- eller anslutningsinstrument.

Artikel 9

Detta avtal kan sägas upp av varje part genom skriftligt meddelande om uppsägning till depositarien, som ska underrätta samtliga andra parter om varje sådant meddelande. Uppsägningen får verkan ett år från det att meddelandet mottagits av depositarien men påverkar inte sådana förpliktelser som redan överenskommit eller de rättigheter och befogenheter som tidigare erhållits av parterna på grundval av bestämmelserna i detta avtal.

Till bekräftelse härav har undertecknade, därtill vederbörligen befullmäktigade av sina respektive regeringar, undertecknat detta avtal.

Upprättat i Bryssel den 6 mars 1997 på engelska och franska språken, vilka båda texter är lika giltiga, i ett enda original som ska deponeras i arkivet hos Amerikas förenta staters regering, som ska sända bestyrkta kopior till var och en av de övriga signatörerna.

Bilaga I

Denna bilaga utgör en integrerad del av avtalet.

När det gäller Natos säkerhetsskyddsklassificerade information

constitutional procedures. Its instrument of accession shall be deposited with the government of the United States of America. It shall enter into force in respect of each acceding State thirty days after the day of the deposit of its instrument of accession.

Article 8

The Government of the United States of America shall inform the Governments of the other Parties of the deposit of each instrument of ratification, acceptance, approval or accession.

Article 9

This Agreement may be denounced by written notice of denunciation by any Party given to the depositary which shall inform all the other Parties of such notice. Such denunciation shall take effect one year after receipt of notification by the depositary, but shall not affect obligations already contracted and the rights or prerogatives previously acquired by the Parties under the provisions of this Agreement.

In witness whereof the undersigned, duly authorized to this effect by their respective Governments, have signed this Agreement.

Done in Brussels, this 6th day of March, 1997 in a single copy in the English and French languages, each text being equally authoritative, which shall be deposited in the archives of the Government of the United States of America and of which certified copies shall be transmitted by that Government to each of the other signatories.

Annex I

This Annex forms an integral part of the Agreement.

NATO classified information is defined as follows:

- a. avses med information kunskap som kan överföras i vilken form som helst, (a) information means knowledge that can be communicated in any form;
- b. avses med säkerhetsskyddsklassificerad information information eller material som kräver skydd mot obehörigt röjande och som med säkerhetsskyddsklassificering har angetts vara sådan, (b) classified information means information or material determined to require protection against unauthorized disclosure which has been so designated by security classification;
- c. innefattar material handlingar samt maskiner, utrustning och vapen som tillverkats eller är under tillverkning, (c) the word "material" includes documents and also any item of machinery or equipment or weapons either manufactured or in the process of manufacture;
- d. avses med handling all lagrad information oavsett fysisk form eller egenskaper, vilket inbegriper men inte inskränker sig till skriftliga dokument och trycksaker, hålkort och hålremсор, kartor, diagram, fotografier, målningar, ritningar, gravyrer, skisser, arbetsanteckningar och arbetsdokument, karbonkopior och färgband, eller återgivningar, oberoende av på vilket sätt eller med vilken metod de görs, samt alla slags ljud- och röstupptagningar, magnetiska, elektroniska och optiska upptagningar och videoupptagningar, bärbar adb-utrustning med fasta lagringsmedier och löstagbara lagringsmedier för datorer. (d) the word "document" means any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable ADP equipment with resident computer storage media, and removable computer storage media.

Bilaga II

Denna bilaga utgör en integrerad del av avtalet.

I detta avtal avses med Nato Nordatlantiska fördragsorganisationen och de organ på vilka tillämpas antingen avtalet om status för Nordatlantiska fördragsorganisationen, nationella representanter och organisationens internationella personal, undertecknat i Ottawa den 20 september 1951, eller protokollet om status för internationella militära högkvarter som inrättats i enlighet med nordatlantiska fördraget, undertecknat i Paris den 28 augusti 1952.

Annex II

This Annex forms an integral part of the Agreement.

For the purposes of the present Agreement, the term "NATO" denotes the North Atlantic Treaty Organization and the bodies governed either by the Agreement on the status of the North Atlantic Treaty Organization, National Representatives and International Staff, signed in Ottawa on 20th September, 1951 or by the Protocol on the status of International Military Headquarters set up pursuant to the North Atlantic Treaty, signed in Paris on 28th August, 1952.

Bilaga III

Denna bilaga utgör en integrerad del av avtalet.

Samråd hålls med militära befälhavare för att respektera deras befogenheter.

Annex III

This Annex forms an integral part of the Agreement.

Consultation takes place with military commanders in order to respect their prerogatives.

NATO UNCLASSIFIED
PUBLICLY DISCLOSED – PDN(2021)0002

Den 20 november 2020

HANDLING
C-M(2002)49-REV1

20 November 2020

DOCUMENT
C-M(2002)49-REV1

**SÄKERHET INOM NORDATLAN-
TISKA FÖRDRAGSORGANISAT-
TIONEN (NATO)**

**Meddelande från generalsekreteraren
Första revideringen av C-M(2002)49 av
den 17 juni 2002**

Referens: C-M(2002)49-COR1-COR12
(konsoliderad version), daterad den 17 juni
2002

1. Denna handling är godkänd av säkerhets-
kommittén och resultatet av en betydande
och övergripande översyn av Natos säker-
hetsstrategi och dess stödjande direktiv.

2. Genom C-M(2002)49-REV1, som ersätter
den handling som nämns i referensen, görs
ändringar i både strukturen och innehållet.

3. Strukturen har ändrats genom att en ny bi-
laga H, i vilken särskilt säkerheten i förbin-
delserna med enheter som inte hör till Nato
behandlas, har fogats till. Denna fråga be-
handlas ytterligare i Natos nyligen utarbe-
tade direktiv om säkerhet i förbindelserna
med enheter som inte hör till Nato (referens
AC/35-D/2006) och i den reviderade stöd-
jande handlingen om säkerhet i förbindel-
serna med Nato för enheter som inte hör till
Nato (referens AC/35-D/1038-REV3) som
stöder direktivet och som är riktad till en-
heter som inte hör till Nato.

4. När det gäller innehållet har vid översyn-
en avsnitt "Grundläggande principer, mini-
normer och ansvar" (bilaga B) samt be-
stämmelser i avsnitten "Personalsäkerhet",
"Fysisk säkerhet", "Informationssäkerhet"
och "Säkerhet i förbindelserna med enheter
som inte hör till Nato" (bilagorna B, C, D, E
och H) ändrats. Vid översynen gjordes inga

**SECURITY WITHIN THE NORTH AT-
LANTIC TREATY ORGANIZATION
(NATO)**

**Note by the Secretary General
Revision 1 to C-M(2002)49 dated 17 June
2002**

Reference: C-M(2002)49-COR1 to COR12
(consolidated version), dated 17 June 2002

1. This document is the result of a major and
comprehensive review of the NATO
Security Policy and its supporting directives,
as approved by the Security Committee.

2. C-M(2002)49-REV1, which replaces the
document at reference, introduces both
structural and content changes.

3. The structure has changed with the addi-
tion of a new Enclosure H to address
specifically security in relation to non-
NATO entities. This topic is developed fur-
ther into the newly developed Directive for
NATO on Security in Relation to Non-
NATO Entities (reference AC/35-D/2006)
and the revised Supporting Document for
Non-NATO Entities on Security in Relation
to NATO (reference AC/35-D/1038-REV3).

4. In terms of content, this revision has ad-
dressed Basic Principles, Minimum
Standards and Responsibilities (Enclosure
B), as well as provisions of Personnel Secu-
rity, Physical Security, Security of Infor-
mation and Security in Relation to Non
NATO Entities (Enclosures B, C, D, E and

56/2023

ändringar i bilagorna F och G till C-M(2002)49.

(Underskrift) Jens Stoltenberg

Bilaga 1
Bilagorna A, B, C, D, E, F, G, H
Ordlista

Originalspråk: engelska

H). Enclosures F and G to C-M(2002)49 were not subject to this review.

(Signed) Jens Stoltenberg

1 Annex
Enclosures A,B,C,D,E,F,G,H
1 Glossary

Original: English

SÄKERHET INOM NORDATLANTISKA FÖRDRAGSORGANISATIONEN (NATO)**SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION (NATO)****INLEDNING**

1. I denna C-M-handling med rubriken Säkerhet inom Nordatlantiska fördragsorganisationen (Nato) återges de grundläggande principer och de miniminormer för säkerhet som ska tillämpas av Natos medlemsstater och Natos civila och militära organ för att säkerställa en gemensam skyddsnivå för säkerhetsskyddsklassificerad information. Natos säkerhetsförfaranden fungerar på bästa möjliga sätt endast när de bygger på och stöds av ett nationellt säkerhetssystem med egenskaper som är likvärdiga eller förenliga med dem som fastställs i denna strategi. Dessutom tas i denna strategi också upp roller, uppgifter och ansvar i fråga om säkerheten inom Nato.

2. Denna handling består av säkerhetsavtalet i bilaga A med namnet "avtal mellan parterna i nordatlantiska fördraget om informationssäkerhet" samt följande bilagor:

- a) Bilaga A — Avtal mellan parterna i nordatlantiska fördraget om informationssäkerhet
- b) Bilaga B — Grundläggande principer, miniminormer och ansvar
- c) Bilaga C — Personalsäkerhet
- d) Bilaga D — Fysisk säkerhet
- e) Bilaga E — Säkerhet för Natos säkerhetsskyddsklassificerade information
- f) Bilaga F — Säkerhet i kommunikations- och informationssystem
- g) Bilaga G — Säkerhetsskyddsklassificerade projekt och industrisäkerhet
- h) Bilaga H — Säkerhet i förbindelserna med enheter som inte hör till Nato.

INTRODUCTION

1. This C-M, entitled Security Within the North Atlantic Treaty Organization (NATO), establishes the basic principles and minimum standards of security to be applied by NATO Nations and NATO Civil and Military bodies in order to ensure a common degree of protection for classified information. NATO security procedures only operate to the best advantage when they are based upon and supported by a national security system having the characteristics equivalent/conformant to those set out in this policy. In addition, this policy also addresses the security roles, functions and responsibilities within NATO.

2. This policy document consists of the Security Agreement at Enclosure "A" entitled "Agreement between the Parties to the North Atlantic Treaty for the Security of Information" together with the following additional Enclosures:

- (a) Enclosure A – Agreement between the parties to NATO for the Security of Information
- (b) Enclosure B – Basic Principles, Minimum Standards and Responsibilities.
- (c) Enclosure C – Personnel Security.
- (d) Enclosure D – Physical Security.
- (e) Enclosure E – Security of NATO Classified Information.
- (f) Enclosure F – Communication and Information System Security.
- (g) Enclosure G – Classified Project and Industrial Security.
- (h) Enclosure H – Security in relation to non-NATO entities.

3. Denna handling stöder strategin för hantering av Natoinformation (C-M(2007)0118). I strategin för hantering av icke-säkerhets-skyddsklassificerad Natoinformation (C-M(2002)60) behandlas de grundläggande principer och normer som ska tillämpas i Natos civila och militära organ och Natos medlemsstater för att skydda icke-säkerhets-skyddsklassificerad Natoinformation (NATO UNCLASSIFIED samt offentlig information).

MÅL OCH MÅLSÄTTNINGAR

4. Natos medlemsstater och Natos civila och militära organ ska se till att de grundläggande principer och miniminormer för säkerhet som återges i denna C-M-handling tillämpas så att Natos säkerhetsskyddsklassificerade information skyddas mot förlust av konfidentialitet, riktighet och tillgänglighet.

5. Natos medlemsstater och Natos civila och militära organ ska utarbeta säkerhetsprogram som följer dessa grundläggande principer och miniminormer så att en gemensam skyddsnivå för Natos säkerhetsskyddsklassificerade information säkerställs.

TILLÄMPNINGSSOMRÅDE

6. Dessa grundläggande principer och miniminormer ska tillämpas på

- a) säkerhetsskyddsklassificerad information som härrör från Nato,
- b) säkerhetsskyddsklassificerad information som härrör från en medlemsstat i Nato och som tillhandahålls Nato eller en annan medlemsstat i Nato som stöd för Natoprogram, Natoprojekt eller Natokontrakt,
- c) säkerhetsskyddsklassificerad information som utbyts mellan Nato och enheter som inte hör till Nato¹, och

3. This policy document supports the NATO Information Management Policy (C-M(2007)0118). The Policy on Management of Non-Classified NATO Information (C-M(2002)60) addresses the basic principles and standards to be applied within NATO Civil and Military bodies and NATO Nations for the protection of Non-Classified NATO information (NATO UNCLASSIFIED and Information releasable to the Public).

AIMS AND OBJECTIVES

4. NATO Nations and NATO Civil and Military bodies shall ensure that the basic principles and minimum standards of security set forth in this C-M are applied to safeguard NATO Classified Information from loss of confidentiality, integrity and availability.

5. NATO Nations and NATO Civil and Military bodies shall establish security programmes that meet these basic principles and minimum standards to ensure a common degree of protection for NATO Classified Information.

APPLICABILITY

6. These basic principles and minimum standards shall be applied to:

- (a) classified information originated by NATO;
- (b) classified information originated by a NATO Nation which is provided to NATO or provided to another NATO Nation in support of a NATO programme, project, or contract;
- (c) classified information exchanged between NATO and non-NATO entities (NNE)¹; and

¹ Stater utanför Nato samt andra organ som inte hör till Nato (till exempel internationella organisationer) inklusive personer som företräder sådana stater eller organ.

- d) säkerhetsskyddsklassificerad information som anförtros personer och organisationer utanför en regering (eller Natos civila eller militära organ), till exempel konsulter, företag och universitet.
- (d) classified information entrusted to individuals and organizations outside a government (or a NATO Civil or Military body), e.g. consultants, industry, universities.
7. På åtkomst till och skydd av Atomalinformation tillämpas avtalet mellan parterna i nordatlantiska fördraget om samarbete avseende nukleär information (C-M(64)39). Administrativa arrangemang för genomförande av avtalet mellan parterna i nordatlantiska fördraget om samarbete avseende nukleär information (C-M(68)41) ska tillämpas för att säkerställa adekvat behörighetskontroll, hantering och skydd av sådan information.
7. Access to, and the protection of, ATOMAL information are subject to the Agreement between the Parties to the North Atlantic Treaty for Co-operation Regarding Atomic Information (C-M(64)39). The Administrative Arrangements to implement the Agreement between the Parties to the North Atlantic Treaty for Co-operation Regarding ATOMAL Information (C-M(68)41) shall be applied to ensure appropriate access control, handling and protection of such information.
8. Åtkomst till och skydd av information om Förenta staternas gemensamma operativa plan (US-Siop) omfattas av bestämmelserna i C-M(71)27(reviderad), som gäller särskilda förfaranden för hantering av information om Förenta staternas gemensamma operativa plan (US-Siop) i Nato.
8. Access to, and protection of, US-SIOP information are subject to the provisions of C-M(71)27(Revised), "Special Procedures for the Handling of United States Single Integrated Operational Plan (US-SIOP) Information within NATO".
9. Den känsliga karaktären hos information, operationer, källor och metoder i samband med signalspaning (SIGINT) förutsätter tillämpning av strikta säkerhetsbestämmelser och säkerhetsförfaranden som ofta går utöver vad som anges i denna C-M-handling. Därför omfattas åtkomst till och skydd av information, operationer, källor och metoder i fråga om signalspaning av nationella bestämmelser och bestämmelserna i MC 101 (Natos strategi för signalspaning) och i alliansens gemensamma publikation AJP, som redogör för MC 101, samt i den handbok om Sigint-administrationen och Sigint-förfarandena som Natos rådgivande kommitté för signalspaning publicerat.
9. The sensitive nature of Signals Intelligence (SIGINT) information, operations, sources and methods require the application of stringent security regulations and procedures often beyond those set forth in this C-M. Therefore, access to and protection of, SIGINT information, operations, sources and methods are subject to national regulations and the provisions laid down in MC 101 (NATO Signals Intelligence Policy) its companion Allied Joint Publication (AJP) and the NATO Advisory Committee on Signals Intelligence (NACSI) Guide to SIGINT Administration and Procedures.

¹ Non-NATO nations, and other non-NATO bodies (e.g. International Organizations) including individuals representing such nations or bodies.

BEHÖRIGHET

10. Nordatlantiska rådet har godkänt denna handling, som genomför avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet (bilaga A) och som sålunda stärker Natos säkerhetsstrategi.²

AUTHORITY

10. The North Atlantic Council (NAC) has approved this document which implements the Agreement Between the Parties to the North Atlantic Treaty for the Security of Information (reproduced at Enclosure "A"), and thereby establishes NATO Security Policy.²

² Enligt säkerhetskommitténs arbetsordning (C-M(2015)0002) utgörs Natos säkerhetsstrategi av C-M(2002)49 och C-M(2002)50.

² Per Terms of reference for the Security Committee (C-M(2015)0002) NATO Security Policy consists of C-M(2002)49 and C-M(2002)50

BILAGA B
C-M(2002)49-REV1

ENCLOSURE "B"
C-M(2002)49-REV1

**BILAGA B
GRUNDLÄGGANDE PRINCIPER, MI-
NIMINORMER OCH ANSVAR**

**ENCLOSURE "B"
BASIC PRINCIPLES, MINIMUM
STANDARDS AND RESPONSIBILI-
TIES**

GRUNDLÄGGANDE PRINCIPER

1. Följande grundläggande principer är tillämpliga:

a) Natos medlemsstater och Natos civila och militära organ ska se till att de överenskomna miniminormer som fastställs i denna C-M-handling tillämpas så att en gemensam skyddsnivå för säkerhetsskyddsklassificerad information som utbyts mellan parterna säkerställs.

b) Med beaktande av ansvaret för att dela ska säkerhetsskyddsklassificerad information endast spridas utifrån behövsenlig behövrighet¹ till personer som har instruerats om relevanta säkerhetsförfaranden.

c) Endast personer som har godkänts vid en adekvat säkerhetsprövning ska ha åtkomst till information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller högre.

d) Beviljandet av godkänt vid en säkerhetsprövning ska inte betraktas som det sista steget i bedömningen av en persons förutsättningar att få åtkomst till säkerhetsskyddsklassificerad information, utan fortgående personalsäkerhetsförfaranden ska införas för hantering av interna hot².

BASIC PRINCIPLES

1. The following basic principles shall apply:

(a) NATO Nations and NATO Civil and Military bodies shall ensure that the agreed-minimum standards set forth in this C-M are applied to ensure a common degree of protection for classified information exchanged among the parties.

(b) Acknowledging the responsibility to share, classified information shall only be disseminated on the basis of the principle of need-to-know¹ to individuals who have been briefed on the relevant security procedures.

(c) Only appropriately cleared individuals shall have access to information classified-NATO CONFIDENTIAL and above.

(d) The granting of a clearance shall not be considered as a final step in assessing an individual's eligibility for access to classified information but ongoing personnel security procedures, referred to as Aftercare, shall be established in order to address the management of the Insider Threat².

¹ En princip enligt vilken det fattas ett positivt beslut när en potentiell informationsmottagare behöver få åtkomst till, kunskap om eller inneha information för sin tjänsteutövning eller för att tillhandahålla officiella tjänster.

¹ The principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services.

² Ett internt hot orsakas av personal som har privilegierad åtkomst till Natos säkerhetsskyddsklassificerade information och/eller Natos tillgångar på grund av sin uppgift inom organisationen och som följaktligen kan missbruka denna åtkomst för att utplåna, skada, flytta eller röja Natos säkerhetsskyddsklassificerade information och/eller Natos tillgångar antingen med avsikt eller till följd av oaktsamhet.

² Insider Threat is represented by personnel who have privileged access to NATO Classified Information and/or NATO assets by virtue of their role within the organization and could subsequently abuse this access to destroy, damage, remove or disclose NATO Classified Information and/or NATO assets either by intention or negligence.

- e) Natos säkerhetsbyrå (NOS) ska samordna hanteringen av interna hot i samarbete med de behöriga nationella myndigheterna och Natos civila och militära organ.
- (e) The NATO Office of Security (NOS) shall coordinate the management of the Insider Threat in conjunction with the appropriate national authorities and NATO Civil and Military bodies.
- f) Hantering av säkerhetsrisker³ ska vara obligatorisk inom Natos civila och militära organ i enlighet med Natos förfarande för hantering av säkerhetsrisker (AC/35-D/1035). Tillämpning av den är frivillig i Natos medlemsstater. Riskhantering får inte användas för att kringgå säkerhetsstrategin.
- (f) Security risk management³ shall be mandatory within NATO Civil and Military bodies in accordance with the NATO Security Risk Management Process (AC/35-D/1035). Its application within NATO Nations is optional. Risk management shall not be used to circumvent security policy.
- g) Natos medlemsstater och Natos civila och militära organ ska inom sina organisationer upprätta program för utbildning i och medvetenhet om säkerhet och dessa ska behandla alla säkerhetsaspekter i enlighet med punkt l nedan.
- (g) NATO Nations and NATO Civil and Military bodies shall establish Security Education and Awareness Programmes within their organizations addressing all security aspects as described in paragraph (l) below.
- h) Alla misstänkta säkerhetsöverträdelser och läckor av säkerhetsskyddsklassificerad information ska omedelbart rapporteras till den behöriga säkerhetsmyndigheten.
- (h) All suspected Security Breaches and compromise of classified information shall be reported immediately to the appropriate security authority.
- i) När de som informationen härrör från lämnar ut säkerhetsskyddsklassificerad information till Nato och Natos medlemsstater för att stödja Natoprogram, Natoprojekt eller Natokontrakt sker det enligt antagandet att informationen kommer att förvaltas och skyddas i enlighet med strategin för hantering av Natoinformation (NIMP) och Natos säkerhetsstrategi.
- (i) Originators release classified information to NATO and to NATO Nations in support of a NATO programme, project or contract on the understanding that it will be managed and protected in accordance with the NATO Information Management Policy (NIMP) and NATO Security Policy.
- j) Säkerhetsskyddsklassificerad information ska kontrolleras av den som informationen härrör från⁴.
- (j) Classified information shall be subject to Originator Control⁴.

³ Ett systematiskt tillvägagångssätt baserat på bedömning av hot och sårbarheter för att fastställa vilka säkerhetsåtgärder som krävs för att skydda informationen och de stödjande tjänsterna och resurserna. Riskhantering omfattar planering, organisering, styrning och kontroll av de resurser som säkerställer att risken hålls inom godtagbara gränser.

³ A systematic approach to determining which security counter-measures are required to protect information and supporting services and resources, based upon an assessment of the threats and vulnerabilities. Risk management involves planning, organising, directing and controlling resources to ensure that the risk remains within acceptable bounds.

⁴ En princip enligt vilken den stat, Nato eller någon annan organisation, under vars överinseende information har skapats, producerats eller introducerats i Nato, fastställer de regler och krav som tillämpas på användningen av denna information och bestämmer över alla ändringar under informationens hela livscykel.

k) Utlämnandet av Natos säkerhetsskyddsklassificerade information ska ske i enlighet med de fastställda förfarandena och kriterierna för utlämnande, och under alla omständigheter ska all Natos säkerhetsskyddsklassificerade information som lämnas ut skyddas av en nivå som är minst lika strikt som den som anges i denna C-M-handling och de stödjande direktiven.

l) Säkerhetsskyddsklassificerad information ska skyddas genom en väl avvägd uppsättning säkerhetsåtgärder som gäller personalsäkerhet, fysisk säkerhet, informations säkerhet och säkerhet i kommunikations- och informationssystem. När säkerhetsskyddsklassificerad information lämnas till entreprenörer och lämnas ut till enheter som inte hör till Nato ska den också skyddas genom att de förfarandeåtgärder som återges i dessa strategier följs. Dessa krav ska omfatta alla personer som har åtkomst till säkerhetsskyddsklassificerad information, alla medier som innehåller säkerhetsskyddsklassificerad information och alla lokaler och utrymmen där sådan information finns.

m) Organisationer som innehar Natos säkerhetsskyddsklassificerade information ska utveckla mekanismer och förfaranden som säkerställer uppfyllandet av kraven enligt Natos säkerhetsstrategi under exceptionella verksamhetsförhållanden, såsom störningstillstånd. Sådana mekanismer och förfaranden kan tas upp i antingen en plan för verksamhetens kontinuitet eller en återhämtningsplan, beroende på typen av incidens.

SKYDD AV INFORMATION OM VIKTIGA OBJEKT

2. Offentliggörande av information om viktiga civila anläggningar (till exempel försvarsmateriellager eller energilager) av militär betydelse i tider av spänning eller krig kan bidra till ett kinetiskt angrepp eller sabotage genom att potentiella fiender eller

(k) The release of NATO Classified Information shall be in accordance with the established procedures and criteria for the release, and in all cases, a degree of protection, no less stringent than that specified in this C-M and the supporting directives, shall be required for any NATO Classified Information released.

(l) Classified information shall be safeguarded by a balanced set of security measures addressing the following subjects: personnel security, physical security, security of information and security of Communication and Information Systems (CIS). When classified information is provided to contractors and released to non-NATO entities (NNE) it shall also be safeguarded by following the procedural measures set by these policies. These requirements shall extend to all individuals having access to classified information, all media carrying classified information, and to all premises containing such information.

(m) Establishments that hold NATO Classified Information shall develop mechanisms and processes to ensure application of NATO Security Policy requirements under adverse operational conditions, including disruptive incidents. Such mechanisms and processes may be reflected in either a Business Continuity Plan or Disaster Recovery Plan, depending on the nature of the incident.

PROTECTION OF INFORMATION ON KEY POINTS

2. The publication of information about critical civilian installations (e.g. defence supplies, energy supply) of military significance in times of tension or war may assist in the delivery of a kinetic attack or act of sabo-

⁴ The principle by which a nation, NATO, or other organization, under whose authority information has been created, produced, or introduced into NATO, establishes the rules and standards which apply to the use of this information and has authority over any changes throughout information life-cycle.

terrorister kan sammanställa en lista över viktiga objekt och använda den för att identifiera objekt som kan vara sårbara för angrepp. Lämpliga åtgärder ska vidtas för att se till att sådan information inte är fritt tillgänglig och för att på så sätt förhindra att fiender använder den på ett fientligt sätt. Dessutom ska ägare och användare av anläggningar av detta slag vara fullt medvetna om risken för sådan verksamhet mot dem och vidta behövliga åtgärder för att skydda denna information.

SÄKERHETSANSVAR

Nationell säkerhetsmyndighet (NSA)

3. Var och en av Natos medlemsstater ska inrätta en nationell säkerhetsmyndighet med ansvar för säkerheten för Natos säkerhets-skyddsklassificerade information. Den nationella säkerhetsmyndigheten fungerar som den främsta kontaktpunkten för Natos säkerhetsbyrå när det gäller säkerhetsfrågor i Nato. Den nationella säkerhetsmyndigheten kan sedan hänvisa Natos säkerhetsbyrå vidare till den utsedda säkerhetsmyndigheten eller någon annan behörig säkerhetsmyndighet.

4. Den nationella säkerhetsmyndigheten ansvarar för

- a) säkerheten för Natos säkerhetsskyddsklassificerade information i såväl militära som civila nationella byråer och enheter i hemlandet och utomlands,
- b) säkerställandet av att regelbundna och adekvata inspektioner av säkerhetsåtgärderna för skydd av Natos säkerhetsskyddsklassificerade information utförs i alla nationella militära eller civila organisationer på alla nivåer för att fastställa att Natos säkerhetsskyddsklassificerade information skyddas på lämpligt sätt i enlighet med Natos gällande säkerhetsbestämmelser. När det gäller organisationer som innehåller information som säkerhetsskyddsklassificerats som COSMIC TOP SECRET eller Atomalinformation, ska säkerhetsinspektioner utföras minst var 24:e månad, om de inte har utförts av Natos säkerhetsbyrå under denna period,

tage by allowing potential enemies or terrorists to compile a key points list, and to use this in order to identify points which may be vulnerable to attack. Appropriate steps shall be taken to ensure that such information is not freely available in the public domain in order to prevent its use in a hostile manner by enemies. Additionally, installations' owners and operators shall be fully aware of the risk of such activity against them and take such steps as necessary to protect this information.

SECURITY RESPONSIBILITIES

National Security Authority (NSA)

3. Each NATO Nation shall establish a National Security Authority (NSA) responsible for the security of NATO Classified Information. The NSA serves as the main point of contact for the NOS for any matter relating to security within NATO. Thereafter, the NSA may direct the NOS to the appropriate Designated Security Authority (DSA) or other competent security authority.

4. The NSA is responsible for:

- (a) the security of NATO Classified Information in national agencies and elements, military or civil, at home or abroad;
- (b) ensuring that periodic and appropriate inspections of the security arrangements for the protection of NATO Classified Information are undertaken in all national organizations at all levels, both military and civil, to determine that NATO Classified Information is appropriately protected in accordance with current NATO security regulations. In the case of organizations holding CTS or ATOMAL information, security inspections shall be made at least every 24 months, unless, during that period, they are carried out by the NOS;

c) säkerställandet av att alla medborgare som behöver åtkomst till information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller högre har beviljats godkänt vid en säkerhetsprövning av person (PSC) i enlighet med Natos säkerhetsstrategi,

d) säkerställandet av att säkerhetsplaner har utarbetats för att förhindra att Natos säkerhetsskyddsklassificerade information hamnar i obehöriga eller fiendliga händer i händelse av en nödsituation, och

e) godkännandet av att nationella Cosmic-centralregister inrättas eller avvecklas. Inrättandet eller avvecklingen av Cosmic-centralregister ska anmälas till Natos säkerhetsbyrå.

Utsedd säkerhetsmyndighet (DSA)

5. En myndighet som ansvarar för att informera industrin om den nationella strategin i alla frågor som gäller Natos industrisäkerhetsstrategi och för att ge ledning och bistånd vid dess genomförande. I vissa medlemsstater kan en utsedd säkerhetsmyndighets verksamhet utföras av den nationella säkerhetsmyndigheten.

Säkerhetskommittén (SC)

6. Säkerhetskommittén är inrättad av Nordatlantiska rådet och består av företrädare för Natos varje medlemsstats nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet, och vid behov får kommittén hjälp av annan säkerhetspersonal från Natos medlemsstater. Företrädare för den internationella militära staben (IMS), de militärstrategiska ledningsinstanserna (ACO och ACT) samt konsultations- och ledningsnämnden (C3B) ska närvara vid säkerhetskommitténs möten. Företrädare för Natos civila och militära organ får också närvara när frågor av intresse för dem tas upp. Natos säkerhetsbyrå utser säkerhetskommitténs ordförande för kommitténs sammansättning av huvudsakliga företrädare, sammansättning som behandlar säkerhetsstrategier samt sammansättning som behandlar säkerhet i kommunikations- och informationssystem.

(c) ensuring that a Personnel Security Clearance (PSC) has been granted to all nationals who are required to have access to information classified NATO CONFIDENTIAL and above, in accordance with NATO Security Policy;

(d) ensuring that security plans have been prepared in order to prevent NATO Classified Information from falling into unauthorised or hostile hands in the event of an emergency; and

(e) authorising the establishment (or dis-establishment) of national COSMIC Central Registries. The establishment (or dis-establishment) of COSMIC Central Registries shall be notified to the NOS.

Designated Security Authority (DSA)

5. An authority responsible for communicating to industry the national policy in all matters of NATO industrial security policy and for providing direction and assistance in its implementation. In some nations, the function of a DSA may be carried out by the NSA.

Security Committee (SC)

6. The SC is established by the North Atlantic Council (NAC) and is composed of representatives from each NATO Nation's NSAs/DSAs and supported, where required, by additional NATO Nation security staff. Representatives of the International Military Staff (IMS), Strategic Commands and Consultation Command and Control (C3) Board shall be present at the meetings of the SC. Representatives of NATO Civil and Military bodies may also be present when matters of interest to them are addressed. The Chairpersons for the SC at Principal's level, the SC in Security Policy Format (SC (SP)), and the SC in Communications and Information Systems (CIS) Security Format (SC (CISS)) are provided by the NOS.

7. Säkerhetskommittén lyder direkt under Nordatlantiska rådet när det gäller

- a) revidering av Natos säkerhetsstrategi (C-M(2002)49 och C-M(2002)50) och givande av rekommendationer om ändring eller godkännande av strategin till Nordatlantiska rådet,
- b) behandling av frågor som gäller Natos säkerhetsstrategi,
- c) översyn och godkännande av de stödjande direktiv och styrdokument som publicerats som stöd för Natos säkerhetsstrategi⁵, och
- d) säkerhetsfrågor som hänvisats till den av Nordatlantiska rådet, en medlemsstat i Nato, generalsekreteraren, militärkommittén (MC), samråds- och ledningsnämnden (C3B) eller någon av cheferna för Natos civila och militära organ och som säkerhetskommittén utarbetar lämpliga rekommendationer om.

Natos säkerhetsbyrå (NOS)

8. Natos säkerhetsbyrå är inrättad vid Natos internationella stab som en del av den gemensamma underrättelse- och säkerhetsavdelningen. Säkerhetsbyrån består av personal med erfarenhet av säkerhetsfrågor inom både militära och civila områden. Den upprätthåller nära förbindelser med nationella säkerhetsmyndigheter eller utsedda säkerhetsmyndigheter i Natos medlemsstater och Natos civila och militära organ. Natos säkerhetsbyrå kan också vid behov begära att Natos medlemsstater och Natos civila och militära organ tillhandahåller ytterligare säkerhetsexperter för att bistå Natos säkerhetsbyrå på deltid när bistånd på heltid inte skulle vara motiverat.

9. Natos säkerhetsbyrå ansvarar för att

- a) behandla eventuella frågor som påverkar Natos säkerhet,
- b) identifiera sätt att förbättra Natos säkerhet,

7. The SC is responsible directly to the NAC for:

- (a) reviewing NATO Security Policy (as set forth in C-M(2002)49 and C-M(2002)50) and making recommendations for change or endorsement to the NAC;
- (b) examining questions concerning NATO Security Policy;
- (c) reviewing and approving the supporting directives and guidance documents published in support of NATO Security Policy;⁵ and
- (d) considering security matters referred to it by the NAC, a NATO Nation, the Secretary General, the Military Committee (MC), the C3 Board or the heads of NATO Civil and Military bodies and preparing appropriate recommendations thereon.

NATO Office of Security (NOS)

8. The NOS is established within the NATO International Staff as part of the Joint Intelligence and Security Division. It is composed of personnel experienced in security matters in both military and civil spheres. The NOS maintains close liaison with the NSAs/DSAs of NATO Nations, and with NATO Civil and Military bodies. The NOS may also, as required, request NATO Nations and NATO Civil and Military bodies to provide additional security experts to assist it for limited periods of time when full-time additions to the NOS would not be justified.

9. The NOS is responsible for:

- (a) examining any questions affecting NATO security;
- (b) identifying means whereby NATO security might be improved;

⁵ En medlemsstat i Nato får begära att ett stödjande direktiv också godkänns av Nordatlantiska rådet.

⁵ A NATO Nation may request that a supporting directive also be approved by the NAC.

c) övergripande samordna säkerheten i Nato mellan Natos medlemsstater och Natos civila och militära organ,

d) säkerställa genomförandet och tillsynen av Natos säkerhetsstrategi, inbegripet givandet av sådana råd som Natos medlemsstater och Natos civila och militära organ begär antingen när det gäller tillämpningen av de grundläggande principer och de säkerhetsnormer som återges i denna bilaga eller vid uppfyllandet av de särskilda säkerhetskraven,

e) i förekommande fall informera säkerhetskommittén, generalsekreteraren och ordföranden för militärkommittén om säkerhetsläget i Nato och om de framsteg som gjorts vid genomförandet av Nordatlantiska rådets säkerhetsbeslut,

f) utföra regelbundna inspektioner av säkerhetssystemen för skydd av Natos säkerhetsskyddsklassificerade information i Natos medlemsstater, Natos civila organ, Natos militärstrategiska högkvarter i Europa (SHAPE) och Natos militärstrategiska högkvarter för transformation (HQ SACT)⁶.

g) genomföra säkerhetskartläggningar i enheter som inte hör till Nato och med vilka Nato har slutit ett säkerhetsavtal först i certifieringssyfte och därefter regelbundet för att säkerställa att Natos säkerhetsstrategi följs,

h) tillsammans med nationella säkerhetsmyndigheter eller utsedda säkerhetsmyndigheter och Natos civila och militära organ samordna utredningen av fall som gäller faktisk eller misstänkt förlust eller läcka av Natos säkerhetsskyddsklassificerade information,

(c) the overall co-ordination of security for NATO among NATO Nations and NATO Civil and Military bodies;

(d) ensuring the implementation and oversight of NATO Security Policy, including the provision of such advice as may be requested by NATO Nations and NATO Civil and Military bodies either in their application of the basic principles and the standards of security described in this Enclosure, or in the implementation of the specific security requirements;

(e) informing, as appropriate, the SC, the Secretary General and the Chair of the MC of the state of security within NATO, and the progress made in implementing NAC decisions regarding security;

(f) carrying out periodic inspections of security systems for the protection of NATO Classified Information in NATO Nations, NATO Civil bodies, SHAPE and HQ SACT;⁶

(g) conducting security surveys in NNEs with whom NATO has a signed Security Agreement for the initial purpose of certification and periodically thereafter for ensuring ongoing compliance with NATO Security Policy;

(h) co-ordinating, with NSAs/DSAs and NATO Civil and Military bodies, the investigation of cases relating to the actual or suspected loss or compromise of NATO Classified Information;

⁶ Natos medlemsstater kan på begäran av Natos säkerhetsbyrå delta i Natos säkerhetsbyrås inspektioner i Natos civila och militära organ antingen som observatörer eller som aktiva medlemmar av inspektionsgruppen. Detta är dock inte möjligt i sådana civila organ där alla av Natos medlemsstater inte är företrädare.

⁶ NATO Nations may, upon request of the NOS, participate in the NOS' inspections to NATO Civil and Military bodies either as observers or as active members of the inspection team. However, this is not possible for civil bodies where not all NATO Nations are part of the constituting framework.

i) vid behov informera nationella säkerhetsmyndigheter eller utsedda säkerhetsmyndigheter om all negativ information som kommer fram och gäller deras medborgare,

j) utarbeta säkerhetsåtgärder för skydd av Natos högkvarter i Bryssel och se till att de genomförs korrekt, och

k) övervaka under ledning av och på generalsekreterarens vägnar genomförandet av Natos säkerhetsprogram för skydd av Atomalinformation i enlighet med bestämmelserna i avtalet (C-M(64)39) och i de stödjande administrativa arrangemangen (C-M(68)41).

(i) informing NSAs/DSAs of any adverse information which comes to light concerning their nationals, where appropriate;

(j) devising security measures for the protection of the NATO Headquarters, Brussels and ensuring their correct implementation; and

(k) supervising, under the direction and on behalf of the Secretary General, the application of the NATO security programme for the protection of ATOMAL information under the provisions of the Agreement (C-M(64)39) and the supporting Administrative Arrangements (C-M(68)41).

Militärkommittén och Natos militära organ

10. Som den högsta militära myndigheten i Nato ansvarar militärkommittén för den övergripande ledningen av militära angelägenheter. Militärkommittén ansvarar följaktligen för alla säkerhetsfrågor i Natos militära struktur, inklusive det centraliserade och övergripande fastställandet av de åtgärder som krävs för att säkerställa att den kryptografiska teknik och det kryptografiska material som används för att överföra Natos säkerhetsskyddsklassificerade information, vilket inbegriper säkerhetsgodkännandet av Natofinansierad kryptografiska utrustning i enlighet med bilaga F till denna C-M-handling. I enlighet med tidigare överenskomna strategier och i överensstämmelse med punkterna 8 och 9 säkerställer Natos säkerhetsbyrå genomförandet av säkerhetsfunktionerna inom Natos militära struktur och håller militärkommitténs ordförande informerad.

11. Cheferna för de militära organ i Nato som är underställda militärkommittén ansvarar för alla säkerhetsfrågor inom sina organisationer. Detta inbegriper ansvar för att se till att en säkerhetsorganisation inrättas, att lämpliga säkerhetsåtgärder och säkerhetsförfaranden utformas och genomförs i enlighet

Military Committee and NATO Military bodies

10. As the highest military authority in NATO, the MC is responsible for the overall conduct of military affairs. The MC is consequently responsible for all security matters within the NATO military structure including centralised overall cognisance of measures necessary to assure the adequacy of cryptographic techniques and materials used for transmitting NATO Classified Information, including the security approval of NATO funded cryptographic equipment as defined in Enclosure "F" to this C-M. In accordance with previously agreed policy and in compliance with paragraphs 8 and 9 above, the NOS carries out the executive functions for security within the NATO military structure and keeps the Chair of the MC informed.

11. The Heads of NATO Military bodies established under the auspices of the MC are responsible for all security matters within their establishments. This includes the responsibility for ensuring that a security organization is set up, that appropriate security measures and procedures are devised and executed in accordance with NATO Security

med Natos säkerhetsstrategi och att säkerhetsåtgärderna regelbundet inspekteras på varje organisationsnivå. När det gäller organisationer som innehåller information som säkerhetsskyddsklassificerats som COSMIC TOP SECRET eller Atomalinformation, ska säkerhetsinspektioner utföras minst var 24:e månad, om inte Natos säkerhetsbyrå har utfört en inspektion under denna period.

Natos civila organ

12. Natos internationella stab och Natos civila byråer ansvarar inför Nordatlantiska rådet för att upprätthålla säkerheten inom sin respektive organisation. Detta innebär ansvar för att se till att en säkerhetsorganisation inrättas, att säkerhetsprogram utformas och genomförs i enlighet med Natos säkerhetsstrategi och att säkerhetsåtgärderna regelbundet inspekteras på varje organisationsnivå. När det gäller organisationer som innehåller information som säkerhetsskyddsklassificerats som COSMIC TOP SECRET eller Atomalinformation, ska säkerhetsinspektioner utföras minst var 24:e månad, om inte Natos säkerhetsbyrå har utfört en inspektion under denna period.

SÄKERHETSTILLSYN I FRÅGA OM KOMPETENSCENTRUM (COE)⁷ /SAMFÖRSTÅNDSAVTALSORGAN

13. Med säkerhetstillsyn avses en tillsynsfunktion för säkerställande av att alla organisationer som hanterar Natos säkerhetsskyddsklassificerade information korrekt tillämpar Natos säkerhetsstrategi när informationen skyddas. När det gäller att skydda Natos säkerhetsskyddsklassificerade information ska säkerhetstillsynen för organ som finns utanför Natos kommandostruktur (NCS) ske enligt följande:

- a) De deltagande medlemsstaterna ansvarar för säkerheten i Natos militära organ (NMB) i fråga och ska vidta lämpliga åtgärder för att säkerställa den. Om det inte

Policy and that the security measures are inspected periodically at each command level. In cases where organizations hold COSMIC TOP SECRET (CTS) or ATOMAL information, security inspections are to be made at least every 24 months, unless, during that period, an inspection has been carried out by the NOS.

NATO Civil bodies

12. The NATO International Staff and NATO civil agencies are responsible to the NAC for the maintenance of security within their establishment. This includes responsibility for ensuring that a security organization is set up, that security programmes are devised and executed in accordance with NATO Security Policy and that the security measures are inspected periodically at each command level. In cases of organizations holding CTS or ATOMAL information, security inspections are to be made at least every 24 months, unless, during that period, an inspection has been carried out by the NOS.

SECURITY OVERSIGHT FOR CENTRE OF EXCELLENCE (COE)⁷ / MEMORANDUM OF UNDERSTANDING (MOU) BODIES

13. Security oversight is defined as the supervisory function to ensure that any organization which handles NATO Classified Information is correctly applying NATO Security Policy for the protection of such information. Security oversight for bodies that lie outside the NATO Command Structure (NCS) in respect of protecting NATO Classified Information shall be delivered as follows:

- (a) Participating nations are responsible and shall make appropriate arrangements as to how to deal with security within

⁷ Samförståndsavtalsorgan godkända av Nordatlantiska rådet i enlighet med PO(2020)0038 (INV).

⁷ NAC-approved COEs in accordance with PO(2020)0038 (INV).

finns särskilda överenskommelser om hur säkerhetstillsynen i dessa enheter ska ske, ska den medlemsstat där enheten/enheterna finns, det vill säga värdstaten, leda säkerhetstillsynen.

b) Kompetenscentrumen/samförståndsavtalsorganen kan vara Natos militära organ, om Nordatlantiska rådet har fattat ett beslut om aktivering i frågan. I sådana fall är Natos säkerhetsstrategi tillämplig och chefen för kompetenscentrumet/samförståndsavtalsorganet ska ansvara för alla säkerhetsfrågor inom sin organisation. De deltagande medlemsstaterna ansvarar för uppfyllandet av säkerhetskraven i kompetenscentrumet/samförståndsavtalsorganet i fråga och ska vidta behövliga åtgärder med avseende på det. Värdstaten ska leda utförandet av säkerhetstillsynen, om inte de deltagande staterna har kommit överens om alternativa arrangemang för denna tillsyn.

c) Om ett kompetenscentrum/samförståndsavtalsorgan inte aktiverats som Natos militära organ (och sålunda inte beviljats internationell status av Nordatlantiska rådet), utan ackrediterats som Natos kompetenscentrum/samförståndsavtalsorgan, tillämpas Natos säkerhetsstrategi. Trots att de deltagande medlemsstaterna ansvarar för alla säkerhetsfrågor inom kompetenscentrumet/samförståndsavtalsorganet, ska värdstaten leda säkerhetstillsynen, om inte de deltagande staterna har kommit överens om alternativa arrangemang för denna tillsyn. I ett samförståndsavtal om inrättande av ett kompetenscentrum/samförståndsavtalsorgan ska det anges hur tillsynen genomförs i kompetenscentrumet/samförståndsavtalsorganet.

d) Om en multinationell enhet i en av Natos medlemsstater varken ackrediterats som kompetenscentrum eller aktiverats som Natos militära organ men använder Natos säkerhetsskyddsklassificerade information, tillämpas Natos säkerhetsstrategi och de deltagande staterna förblir ansvariga för säkerhetsfrågorna. Om det

their NATO Military Body (NMB). Unless there are specific agreements in place regarding how to deal with security oversight for these elements, the Nation in which the element(s) is/are situated, i.e. the Host Nation, shall take the lead for exercising security oversight.

(b) COE/MOU bodies can be NMB if there is a NAC activating decision. In such cases NATO Security Policy is applicable and the head of the COE/MOU body shall be responsible for all security matters within their establishment. Participating nations are responsible and shall make necessary arrangements to deal with security requirements within any COE/MOU body. The Host Nation shall take the lead for exercising security oversight unless participating nations have agreed to alternative arrangements for this oversight.

(c) If a COE/MOU body is not activated as a NMB (and thus not granted international status by the NAC), but accredited as a NATO COE/MOU, NATO Security Policy applies. Although participating nations will be responsible for all security matters within the COE/MOU, the Host Nation shall take the lead for exercising security oversight unless participating nations have agreed to alternative arrangements for this oversight. Any founding MOU shall describe how this is implemented within the COE/MOU body.

(d) If a multi-national entity within one of the NATO Nations is not accredited as a COE, nor activated as a NMB but uses NATO Classified Information, NATO Security Policy applies and the participating nations remain responsible for security matters. If there are non-NATO nations participating, a security agreement

finns stater utanför Nato som deltar, måste ett säkerhetsavtal slutas med dessa stater innan säkerhetsskyddsklassificerad information kan utbytas. I dessa fall ska värdstaten leda säkerhetstillsynen, om inte de deltagande staterna har kommit överens om alternativa arrangemang för denna tillsyn. I ett samförståndsavtal om inrättande av en multinationell enhet ska det anges hur tillsynen genomförs i den multinationella enheten.

with those nations must be in place before classified information can be exchanged. In such circumstances the Host Nation shall take the lead for security oversight unless participating nations have agreed to alternative arrangements for this oversight. Any founding MOU shall describe how this is implemented within the multi-national entity.

SÄKERHETSSAMORDNING

14. Alla Natosäkerhetsfrågor mellan nationella säkerhetsmyndigheter eller utsedda säkerhetsmyndigheter i Natos medlemsstater och mellan Natos civila och militära organ som inte kan lösas, eller alla frågor om genomförande eller tolkning av Natos säkerhetsstrategi, ska hänvisas till Natos säkerhetsbyrå. Om en sådan hänvisning görs av militära myndigheter ska den ske via ordervägar. Eventuella olösta meningsskiljaktigheter ska av Natos säkerhetsbyrå hänvisas till säkerhetskommittén för behandling.

SECURITY CO-ORDINATION

14. Any NATO security issue between NSAs/DSAs of NATO Nations, and NATO Civil and Military bodies that cannot be resolved, or any issue with implementing or interpreting NATO Security Policy, shall be referred to the NOS. In cases where such reference is by military authorities, this shall be made through command channels. Any unresolved differences shall be submitted by the NOS to the SC for consideration.

ÄNDRINGAR AV SÄKERHETSSTRATEGIN

15. Natos medlemsstaters och Natos civila och militära organs förslag till ändring av Natos säkerhetsstrategi ska i första hand hänvisas till Natos säkerhetsbyrå. Alla förslag som läggs fram av militära myndigheter ska förmedlas via ordervägar. Förslagen behandlas av Natos säkerhetsbyrå och vid behov läggs de fram för säkerhetskommittén för fortsatt behandling. Denna punkt utesluter inte att nationella säkerhetsmyndigheter eller utsedda säkerhetsmyndigheter i Natos medlemsstater formellt lägger fram förslag för säkerhetskommittén, om de så önskar.

SECURITY POLICY MODIFICATIONS

15. Any proposals by NATO Nations and NATO Civil and Military bodies to modify NATO Security Policy should be referred in the first instance to the NOS. Any proposals made by the military authorities shall be transmitted through command channels. Proposals will be considered by the NOS and if necessary raised to the SC for further discussion. This paragraph does not preclude the NSAs/DSAs from NATO Nations formally making proposals to the SC if they wish.

BILAGA C
C-M(2002)49-REV1

ENCLOSURE "C"
C-M(2002)49-REV1

**BILAGA C
PERSONALSÄKERHET**

INLEDNING

1. I denna bilaga presenteras strategin och miniminormerna för personalsäkerhet. Ytterligare detaljer och krav finns i det stödjande direktivet om personalsäkerhet (AC/35-D/2000).
2. Personalsäkerhetsförfarandena ska utformas så att det genom dem fastställs huruvida personen i fråga, med beaktande av hur lojal, tillförlitlig och pålitlig personen är, kan ges behörighet att få åtkomst till säkerhetskyddsklassificerad information utan att detta medför en oacceptabel säkerhetsrisk. Detta förutsätter att alla civila och militära personer¹, vars plikter eller uppgifter kräver åtkomst till information som säkerhetskyddsklassificerats som CONFIDENTIAL² eller högre, ska prövas på adekvat sätt så att man erhåller tillräckligt förtroende för deras lämplighet att få åtkomst till sådan information och därmed för innehav av ett vid en säkerhetsprövning av person beviljat godkännande (PSC).³
3. När det gäller åtkomst till Natos säkerhetskyddsklassificerade information som säkerhetskyddsklassificerats som NATO CONFIDENTIAL eller högre ska personen i

**ENCLOSURE "C"
PERSONNEL SECURITY**

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for Personnel Security. Additional details and requirements are found in the supporting Directive on Personnel Security (AC/35-D/2000).
2. Personnel security processes shall be designed to determine whether an individual can, taking into account their assessed loyalty, trustworthiness and reliability, be authorised to have access to classified information without constituting an unacceptable risk to security. To achieve this, all individuals¹, civilian and military, whose duties or functions require access to information classified CONFIDENTIAL² and above shall be appropriately investigated to give a satisfactory level of confidence as to their eligibility for access to such information and as such possess a national Personnel Security Clearance (PSC).³
3. In terms of access to NATO Classified Information NATO CONFIDENTIAL (NC) and above an individual will require a valid national PSC at the appropriate level along with the confirmation from the appropriate

¹ Med undantag för statens högsta ledning i enlighet med punkt 7 i denna bilaga.

¹ Aside from those Senior Government Officials, referred to in the paragraph 7 of this Enclosure.

² Vissa medlemsstater i Nato kräver i enlighet med sina nationella lagar och regler en godkänd säkerhetsprövning av person (PSC) för åtkomst till information som säkerhetskyddsklassificerats som RESTRICTED eller information på motsvarande nationell nivå.

² Some NATO Nations, as mandated by their national laws and regulations, require a PSC for access to classified information at the level of RESTRICTED or national equivalent.

³ En godkänd säkerhetsprövning av person (PSC) är en positiv bedömning, genom vilken en nationell säkerhetsmyndighet eller en utsedd säkerhetsmyndighet eller någon annan behörig säkerhetsmyndighet formellt erkänner personens lämplighet att få åtkomst till information som säkerhetskyddsklassificerats som NATO CONFIDENTIAL eller högre med hänsyn till individens lojalitet, tillförlitlighet och pålitlighet.

³ A PSC is a positive determination by which an NSA/DSA or other competent security authority formally recognizes the individual's eligibility to have access to information classified NC and above taking into account their loyalty, trustworthiness and reliability.

fråga ha beviljats ett giltigt nationellt godkännande vid en adekvat säkerhetsprövning av person (PSC) samt inneha ett av den behöriga nationella säkerhetsmyndigheten eller den behöriga utsedda säkerhetsmyndigheten eller någon annan behörig säkerhetsmyndighet utfärdat intyg om att personen i fråga kan beviljas åtkomst till Natos säkerhetsskyddsklassificerade information.

TILLÄMPNING AV PRINCIPEN OM BEHOVSENLIG BEHÖRIGHET

4. Personer i Natos medlemsstater och i Natos civila och militära organ ska endast ha åtkomst till sådan av Natos säkerhetsskyddsklassificerade information som de har behovsenlig behörighet för. Ingen har rätt att få åtkomst till Natos säkerhetsskyddsklassificerade information enbart på grundval av ställning eller tjänst eller godkänd säkerhetsprövning av person (PSC).

GODKÄND SÄKERHETSPRÖVNING AV PERSON (PSC)

5. Enligt Natos säkerhetsstrategi krävs det inte en godkänd säkerhetsprövning av person (PSC) för åtkomst till information som säkerhetsskyddsklassificerats som NATO RESTRICTED.⁴ Personer som endast behöver åtkomst till information som säkerhetsskyddsklassificerats som NATO RESTRICTED ska ha informerats om sina säkerhetsåligganden när det gäller skyddet av Natos säkerhetsskyddsklassificerade information⁵, ska skriftligen eller på ett motsvarande sätt som säkerställer oavvislighet ha intygat att de är medvetna om sitt säkerhetsansvar och ska även ha behovsenlig behörighet.

NSA/DSA or other competent security authority that the individual in question may be authorised to access NATO Classified Information.

APPLICATION OF THE NEED-TO-KNOW PRINCIPLE

4. Individuals in NATO Nations and in NATO Civil and Military bodies shall only have access to NATO Classified Information for which they have a need-to-know. No individual is entitled solely by virtue of rank or appointment or PSC to have access to NATO Classified Information.

PERSONNEL SECURITY CLEARANCES (PSCs)

5. A PSC is not required by NATO Security Policy for access to information classified NATO RESTRICTED (NR).⁴ Individuals who only require access to information classified NR shall have been briefed on their security obligations in respect to the protection of NATO Classified Information⁵, shall have acknowledged their security responsibilities in writing or an equivalent method which ensures non-repudiation and shall also have a need-to-know.

⁴ Vissa medlemsstater i Nato kan i enlighet med sina nationella lagar och regler kräva en godkänd säkerhetsprövning av person (PSC) för åtkomst till information som säkerhetsskyddsklassificerats som NATO RESTRICTED.

⁴ Some NATO Nations, in accordance with their national laws and regulations, may require a PSC for access to information classified NR.

⁵ Medlemsstaterna kan använda antingen Natos egna anvisningar eller motsvarande nationella anvisningar, om de senare nämnda belyser skillnaderna mellan kraven i de två säkerhetsramverken.

⁵ Nations may use either NATO specific briefings or national equivalent if the latter highlights the differences between the requirements of the two security frameworks.

6. En godkänd säkerhetsprövning av person (PSC) krävs när personer har åtkomst till information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller högre eller kan få åtkomst till sådan information under sin tjänsteutövning. Dessutom ska personerna ha

- a) behovsenlig behörighet,
- b) informerats om sina säkerhetsåligganden när det gäller skyddet av Natos säkerhetsskyddsklassificerade information,
- c) antingen skriftligen eller genom en motsvarande metod som säkerställer oavvislighet intygat att de är medvetna om sitt ansvar.

7. Med avvikelse från punkterna 5 och 6 fastställs i nationella lagar och regler åtkomst för statens högsta ledning (till exempel stats- och regeringschefer, ministrar, riksdagsledamöter och domstolsväsendets ledamöter) till Natos säkerhetsskyddsklassificerade information; dessa personer ska informeras om sina säkerhetsåligganden och ha behovsenlig behörighet.

8. Nivån på en behövlig godkänd säkerhetsprövning av person (PSC) och därmed omfattningen av de förfaranden för säkerhetsprövning som genomförs ska fastställas utifrån säkerhetsskyddsklassificeringsnivån för Natos säkerhetsskyddsklassificerade information som personen ska ha åtkomst till. Det ska finnas en överenskommen norm för förtroende när det gäller godkännande av de personer som beviljas åtkomst till eller vars tjänsteutövning eller uppgifter kan ge åtkomst till Natos säkerhetsskyddsklassificerade information.

9. Beviljandet av godkänt vid en säkerhetsprövning av person (PSC) ska inte betraktas som det sista steget i personalsäkerhetsförfarandet; det förutsätts säkerställande av att en person fortgående är behörig att få åtkomst till Natos säkerhetsskyddsklassificerade information. Detta uppnås genom att säkerhetsmyndigheter och säkerhetschefer ser till att effektivt delaktiggöra personer och regel-

6. An appropriate PSC is required when individuals access information classified NC and above or may have access to such information during the course of their duties. In addition, individuals are required to:

- (a) have a need-to-know;
- (b) have been briefed on their security obligations in respect to the protection of NATO Classified Information;
- (c) have acknowledged their responsibilities either in writing or an equivalent method which ensures non-repudiation.

7. As an exception to paragraphs 5 and 6 above, access to NATO Classified Information by Senior Government Officials (e.g. Heads of State and Government, Government Ministers, Members of Parliament, Members of the Judiciary) is determined by national laws and regulations; such officials shall be briefed on their security obligations and shall have a need-to-know.

8. The level of PSC required and, therefore, the extent of security clearance processes undertaken shall be determined by the level of classification of the NATO Classified Information to which the individual is to have access. There shall be an agreed standard of confidence regarding the eligibility of individuals granted access to, or whose duties or functions may afford access to, NATO Classified Information.

9. The granting of a PSC should not be considered as a final step in the personnel security process; there is a requirement to ensure an individual's continuing eligibility for access to NATO Classified Information. This is to be achieved through effective engagement and regular evaluation by security authorities and managers. This includes assessing any change in circumstance or behaviour with potential security implications.

bundet bedöma dem. Detta inbegriper bedömning av alla förändringar i omständigheter eller beteenden med potentiella konsekvenser för säkerheten. Dessutom ska program för säkerhetsutbildning och säkerhetsmedvetenhet effektivt användas för att påminna enskilda personer om deras säkerhetsansvar och om behovet av att rapportera till sina chefer eller säkerhetspersonal information som kan påverka deras säkerhetsstatus.

Exceptionella omständigheter

10. Det kan uppstå situationer där vissa av kraven i punkt 6 inte kan uppfyllas till exempel på grund av brådskande uppdrag. Närmare detaljer i fråga om temporära utnämningar, tillfällig åtkomst eller åtkomst i nödsituationer finns i det stödjande direktivet om personalsäkerhet.

Ansvar

11. Den medlemsstat i Nato vars medborgare en ansökan om säkerhetsprövning av person gäller ska behandla ansökan. Detta inbegriper kravet att säkerställa att förfarandet för säkerhetsprövning av person uppfyller minimikraven och minimikriterierna för bedömning av personens lojalitet, tillförlitlighet och pålitlighet när det gäller beviljande av godkänt vid en säkerhetsprövning av person (PSC) samt de krav som gäller förnyelse av ett erhållet godkännande vid en säkerhetsprövning av person i enlighet med direktivet om personalsäkerhet.

12. Natos civila och militära organ ansvarar för inlämning av ansökningar om säkerhetsprövning av person och om förnyelse av ett erhållet godkännande vid en säkerhetsprövning av person för sin personal till den vederbörande nationella säkerhetsmyndigheten eller den vederbörande utsedda säkerhetsmyndigheten eller någon annan behörig säkerhetsmyndighet.

13. Närmare detaljer om det ansvar som nationella säkerhetsmyndigheter eller utsedda säkerhetsmyndigheter eller andra behöriga säkerhetsmyndigheter, Natos medlemsstater och cheferna för Natos civila eller militära

Additionally, the effective use of security education and awareness programme(s) shall be used in order to remind individuals of their security responsibilities and of the need to report, to their managers or security staff, information which may affect their security status.

Exceptional Circumstances

10. Circumstances may arise when, for example for urgent mission purposes, some of the requirements in paragraph 6 above cannot be met. Details in respect to provisional appointments, temporary and emergency access, are set out in the supporting Directive on Personnel Security.

Responsibilities

11. It is the responsibility of the NATO Nation, of which the individual is a national, to process PSC applications. This includes the requirement to ensure that their PSC process meets the minimum investigative requirements and criteria for assessing the loyalty, trustworthiness and reliability of an individual in order to be granted a PSC as well as the requirements for renewal of PSC as set out in the Directive on Personnel Security.

12. NATO Civil and Military bodies are responsible for submitting PSC applications and renewals for their staff to the relevant NSA/DSA or other competent security authority.

13. The detailed responsibilities of NSAs/DSAs or other competent security authorities, NATO Nations and the Heads of a NATO Civil or Military bodies are set out in the Directive on Personnel Security.

organ har fastställs i direktivet om personalsäkerhet.

SÄKERHETSUTBILDNING OCH MEDVETENHET

14. Alla personer med sådana arbetsuppgifter där de har åtkomst till information som säkerhetsskyddsklassificerats som NATO RESTRICTED eller som har godkänts vid en säkerhetsprövning av person (PSC) för åtkomst till NATO CONFIDENTIAL eller högre ska informeras om säkerhetsförfaranden och sina säkerhetsåligganden. Alla personer som har godkänts vid en säkerhetsprövning ska intyga att de fullt ut förstår sitt ansvar och de potentiella konsekvenserna för dem om Natos säkerhetsskyddsklassificerade information hamnar i obehöriga händer antingen uppsåtligt eller genom oaktksamhet. En förteckning över dessa intyganden ska upprätthållas av den medlemsstat eller de civila eller militära organ i Nato som ger åtkomst till Natos säkerhetsskyddsklassificerade information.

15. Alla som är behöriga att ha åtkomst till eller som har till uppgift att hantera Natos säkerhetsskyddsklassificerade information ska inledningsvis göras medvetna om och regelbundet påminnas om de hot mot säkerheten som orsakas av bland annat följande:

- a) personernas uppförande utanför arbetsplatsen, inbegripet användning av sociala medier,
- b) indiskreta samtal med personer utan behovsenlig behörighet,
- c) arbete utanför arbetsplatsen och vid resor,
- d) cyberhot,
- e) personernas förhållande till medierna, och
- f) det hot som underrättelseverksamhet riktad mot Nato och dess medlemsstater utgör.

SECURITY EDUCATION AND AWARENESS

14. All individuals employed in positions where they have access to information classified NR, or hold a PSC for access to NC or above, shall be briefed on security procedures and their security obligations. All cleared individuals shall acknowledge that they fully understand their responsibilities and the potential consequences to them when NATO Classified Information passes into unauthorised hands either by intent or through negligence. A record of the acknowledgement shall be maintained by the NATO Nation or NATO Civil or Military Body authorising access to NATO Classified Information.

15. All individuals who are authorised access to, or are required to handle NATO Classified Information, shall initially be made aware, and periodically reminded of the threats to security arising from but not limited to the following:

- (a) personal conduct outside the office, including activity on social media;
- (b) indiscreet conversations with individuals without the need-to-know;
- (c) working outside the office and when travelling;
- (d) cyber threats;
- (e) their relationship with the media; and
- (f) the threat presented by the activities of intelligence services which target NATO and its Nations.

16. Personerna ska omedelbart rapportera till de behöriga säkerhetsmyndigheterna alla kontakter eller åtgärder som de anser vara misstänkta eller ovanliga.

16. Individuals shall report immediately to the appropriate security authorities any approach or manoeuvre which they consider suspicious or unusual.

BILAGA D
C-M(2002)49-REV1

ENCLOSURE "D"
C-M(2002)49-REV1

**TILLÄGG D
FYSISK SÄKERHET**

INLEDNING

1. I denna bilaga fastställs strategin och miniminormerna för fysiska säkerhetsåtgärder till skydd för Natos säkerhetsskyddsklassificerade information. Ytterligare detaljer och krav finns i det stödjande direktivet om fysisk säkerhet (AC/35-D/2001).

2. Med fysisk säkerhet avses tillämpning av fysiska skyddsåtgärder på platser, byggnader, verksamhetsställen eller anläggningar där det finns säkerhetsskyddsklassificerad information som kräver skydd mot förluster eller läckor.

3. Natos medlemsstater och Natos civila och militära organ ska upprätta fysiska säkerhetsprogram, som omfattar aktiva och passiva säkerhetsåtgärder och som skapar en gemensam nivå av fysisk säkerhet som motsvarar bedömningen av hot mot, sårbarheter hos samt säkerhetsskyddsklassificering och mängd av den information som ska skyddas.

SÄKERHETSKRAV

4. Alla platser, byggnader, verksamhetsställen, kontor, rum och andra utrymmen där Natos säkerhetsskyddsklassificerade information lagras, hanteras och/eller diskuteras ska skyddas genom adekvata fysiska säkerhetsåtgärder. Vid beslut om vilken nivå av fysiskt skydd som behövs ska hänsyn tas till alla relevanta faktorer, såsom

- a) nivån på säkerhetsskyddsklassificerad information samt informationskategori,
- b) mängd och form (pappersform och/eller elektronisk form) av den säkerhetsskyddsklassificerade information som lagras och/eller hanteras,
- c) behörighetskontroll och verkställande av principen om behovsenlig behörighet,

**ENCLOSURE "D"
PHYSICAL SECURITY**

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for physical security measures for the protection of NATO Classified Information. Additional details and requirements are found in the supporting Directive on Physical Security (AC/35-D/2001).

2. Physical security is the application of physical protective measures to sites, buildings, facilities or installations that contain classified information requiring protection against loss or compromise.

3. NATO Nations and NATO Civil and Military bodies shall establish physical security programmes, consisting of active and passive security measures, to provide a common degree of physical security consistent with the assessment of the threats, vulnerabilities, security classification and quantity of the information to be protected.

SECURITY REQUIREMENTS

4. All sites, buildings, facilities, offices, rooms, and other areas in which NATO Classified Information is stored, handled and/or discussed shall be protected by appropriate physical security measures. In deciding what degree of physical security protection is necessary, account shall be taken of all relevant factors, such as:

- (a) the level of security classification and category of information;
- (b) the quantity and form of the classified information (hard copy, and/or electronic) stored, and/or handled;
- (c) access control and enforcement of the need-to-know principle;

d) det hot från fientliga underrättelsetjänster som är riktat mot Nato och/eller dess medlemsstater samt det lokalt bedömda hotet i fråga om terrorism, spionage, sabotage, subversion och (organiserad) brottslighet, och

e) hur den säkerhetsskyddsklassificerade informationen lagras (till exempel i pappersform eller elektronisk form och som krypterad).

5. Fysiska säkerhetsåtgärder ska utformas så att de

a) förhindrar intrång i smyg eller genom tvång,

b) avskräcker, hindrar och avslöjar handlingar i fråga om interna hot,

c) möjliggör olika behandling av personalen med avseende på åtkomst till Natos säkerhetsskyddsklassificerade information utifrån nivån på en godkänd säkerhetsprövning av person (PSC) och principen om behovsenlig behörighet, och

d) så snart som möjligt upptäcker alla säkerhetsincidenter och utifrån dem leder till behövliga åtgärder.

ALLMÄNNA FYSISKA SÄKERHETSKRAV

6. Fysiska åtgärder utgör endast en aspekt av säkerhetsskyddet och ska stödjas av solida säkerhetsåtgärder i fråga om personalsäkerhet, informationssäkerhet samt kommunikations- och informationssystem. Förständig hantering av säkerhetsrisker inbegriper att man fastställer de mest proportionella, effektiva och kostnadseffektiva metoderna för bekämpning av hoten och kompensation av sårbarheter genom en kombination av dessa områdens skyddsåtgärder. En sådan effektivitet och kostnadseffektivitet uppnås bäst genom att i samband med planeringen och utformningen av verksamhetsställen fastställa fysiska säkerhetskrav, vilket minskar behovet av kostsamma renoveringar.

7. Fysiska säkerhetsprogram ska grunda sig på principen om flernivåförsvar och omfatta

(d) the threat from hostile intelligence services which target NATO and/or its member Nations, and the locally-assessed threat of terrorism, espionage, sabotage, subversion and (organized) crime; and

(e) how the classified information will be stored (e.g. hard copy or electronic and encrypted).

5. Physical security measures shall be designed to:

(a) deny surreptitious or forced entry by an intruder;

(b) deter, impede and detect actions from the insider threat;

(c) allow for segregation of personnel in their access to NATO Classified Information in accordance with their level of Personnel Security Clearance (PSC) and the need-to-know principle; and

(d) detect and act upon all security incidents as soon as possible.

GENERAL PHYSICAL SECURITY REQUIREMENTS

6. Physical measures represent only one aspect of protective security and shall be supported by sound personnel security, security of information, and Communication and Information Systems (CIS) security measures. Sensible management of security risks will involve establishing the most proportionate, efficient and cost-effective methods of countering the threats and compensating for vulnerabilities by a combination of protective measures from these domains. Such efficiency and cost-effectiveness is best achieved by defining physical security requirements as part of the planning and design of facilities, thereby reducing the need for costly renovations.

7. Physical security programmes shall be based on the principle of “defence in depth”,

en adekvat kombination av kompletterande fysiska säkerhetsåtgärder som ger den nivå av skydd som uppfyller de krav som hänger samman med hur väsentlig och sårbar organisationen och dess information är.

8. Trots att fysiska säkerhetsåtgärder är platsspecifika och bestäms av ett antal faktorer, ska följande allmänna principer gälla:

- a) först ska de tillgångar som kräver skydd identifieras. Efter det skapas stegvisa säkerhetsåtgärder för att tillhandahålla flernivåförsvar och fördröjande faktorer,
- b) de yttersta fysiska säkerhetsåtgärden ska avgränsa det skyddade utrymmet och förhindra obehörigt tillträde,
- c) nästa åtgärdsnivå ska upptäcka obehörigt tillträde eller försök till tillträde och varna vaktpersonalen, och
- d) den innersta åtgärdsnivån ska fördröja inkräktare tills de kan anhållas av vaktpersonalen. Följaktligen finns det ett inbördes samband mellan vaktpersonalens reaktionstid och de fysiska säkerhetsåtgärder som är avsedda att fördröja inkräktarna.

9. Den utrustning som ger fysisk säkerhet (till exempel övervakningskameror, system för upptäckt av intrång, säkerhetsskåp) ska underhållas regelbundet eller av en specifik orsak för att säkerställa att den fungerar på bästa möjliga sätt. Det är också nödvändigt att regelbundet bedöma effektiviteten hos enskilda säkerhetsåtgärder och hela säkerhetssystemet. Detta är särskilt viktigt om användningen av platsen eller särskilda delar av säkerhetssystemet ändras. Detta kan uppnås genom att regelbundet genomföra övningar på grundval av säkerhetsplanerna.

Säkra utrymmen

10. Permanenta eller tillfälliga utrymmen där information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller högre lagras, hanteras och/eller diskuteras

using an appropriate combination of complementary physical security measures which provide a degree of protection meeting the requirements associated with the criticality and vulnerability of the organization and its information.

8. Although physical security measures are site-specific, and determined by a number of factors, the following general principles shall apply:

- (a) it is first necessary to identify the assets that require protection. This is followed by the creation of layered security measures to provide "defence in depth" and delaying factors;
- (b) the outermost physical security measures shall define the protected area and deter unauthorised access;
- (c) the next layer of measures shall detect unauthorised or attempted access and alert the guard force; and
- (d) the innermost layer of measures shall sufficiently delay intruders until they can be detained by the guard force. Consequently, there is an interrelationship between the reaction time of the guard force and the physical security measures designed to delay intruders.

9. Equipment that provides physical security (e.g. CCTV, IDS, secure cabinets) shall be maintained regularly or in response to a specific cause to ensure that it operates at optimum performance. It is also necessary to periodically re-evaluate the effectiveness of individual security measures as well as the complete security system. This is particularly important if there is a change in use of the site or specific elements of the security system. This can be achieved by regularly exercising security plans.

Security Areas

10. Areas, either fixed or temporary, in which information classified NATO CONFIDENTIAL (NC) and above is stored, handled and/or discussed shall be organised and

ska organiseras och struktureras så att de motsvarar något av följande:

a) **Natos säkra utrymme av klass I:** ett särskilt känsligt utrymme där information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller högre lagras, hanteras och/eller diskuteras på ett sådant sätt att tillträde till utrymmet i praktiken innebär åtkomst till Natos säkerhetsskyddsklassificerade information och obehörigt tillträde därför utgör en säkerhetsöverträdelse.

Utrymmen av detta slag kan inbegripa ledningscentraler, kommunikationscenter eller arkivrum och kräver

- i) en tydlig och skyddad yttre gräns genom vilken alla in- och utpasseringar kontrolleras,
- ii) ett sådant system för behörighetskontroll som endast ger de personer som godkänts vid en adekvat säkerhetsprövning och som har särskilt tillstånd¹ att komma in i utrymmet tillträde,
- iii) ett fastställande av nivån på säkerhetsskyddsklassificeringen och av kategorin av den information som normalt finns i utrymmet, det vill säga den information som tillträdet ger åtkomst till, och
- iv) ett tydligt omnämnande av att tillträde till sådana utrymmen kräver särskilt tillstånd från den lokala säkerhetsmyndigheten. Detta omnämnande kan omfatta säkerhetsskyddsklassificeringens nivå och/eller utrymmets känslighet.

b) **Natos säkra utrymme av klass II:** ett utrymme där information som säkerhets-

structured so as to correspond to one of the following:

(a) **NATO Class I Security Area:** a particularly sensitive area in which information classified NC and above is stored, handled and/or discussed in such a way that entry into the area constitutes, for all practical purposes, access to NATO Classified Information and therefore unauthorised entry would constitute a Security Breach.

Such areas may include operations rooms, communications centres or archive facilities and require:

- (i) a clearly defined and protected perimeter through which all entry and exit is controlled;
- (ii) an entry control system which grants access only to those individuals appropriately cleared and specifically authorised¹ to enter the area;
- (iii) a determination of the level of security classification and the category of the information normally held in the area, i.e. the information to which entry gives access; and
- (iv) a clear indication that entrance into such areas requires specific authorization by the local security authority. This indication may include the level of security classification and/or the sensitivity of the area.

(b) **NATO Class II Security Area:** an area in which information classified NC

¹ Med innehavare av särskilt tillstånd avses personal med formellt erkänd behovsenlig behörighet samt åtkomst till information på grund av arten av sina arbetsuppgifter och som finns på en lista för behörighetskontroll, samt de personer som chefen för organisationen i fråga från fall till fall formellt har befullmäktigat att utföra en viss uppgift.

¹ Specifically authorised refers to those personnel who have been formally recognised as having a need-to-know and access based on the nature of their employment responsibilities, and are included on an access control list, as well as individuals who have been formally authorised by the head of the organization in question on an ad hoc basis to perform a specific role or duty.

skyddsklassificerats som NATO CONFIDENTIAL eller högre lagras, hanteras och/eller diskuteras på ett sådant sätt att obehöriga personers åtkomst till den kan förhindras genom internt inrättade tillsynssystem.

Utrymmen av detta slag kan inbegripa kontor eller sammanträdesrum där Natos säkerhetsskyddsklassificerade information lagras, hanteras och/eller diskuteras.

Dessa utrymmen kräver

- i) en tydlig och skyddad yttre gräns genom vilken alla in- och utpasseringar kontrolleras,
- ii) ett sådant system för behörighetskontroll som ger endast personer som godkänts vid en säkerhetsprövning och som har tillstånd att komma in i utrymmet obeleddat tillträde, och
- iii) en ledsagare eller motsvarande kontrollmekanism när det gäller sådana personer som inte uppfyller kriterierna i underpunkt b ii, så att obehörig åtkomst till Natos säkerhetsskyddsklassificerade information och okontrollerat tillträde till utrymmen som är särskilt fastställda som utrymmen skyddade mot tekniska angrepp och avlyssning förhindras.

Administrativ zon

11. En administrativ zon ska upprättas runt eller leda till Natos säkra utrymmen av klass I eller II. Endast information som säkerhetsskyddsklassificerats som NATO RESTRICTED får lagras, hanteras och/eller diskuteras i administrativa zoner. Utrymmen av detta slag ska ha en synlig yttre gräns, vid vilken det finns möjlighet att kontrollera personer och fordon. Enskilda personer behöver dock inte ledsagare.

Tekniskt säkra utrymmen

12. Permanenta eller tillfälliga tekniskt säkra utrymmen är utrymmen som uttryckligen identifierats kräva skydd mot tekniska angrepp och avlyssning. Dessa utrymmen ska vara föremål för regelbundna fysiska och

and above is stored, handled and/or discussed in such a way that it can be protected from access by unauthorised individuals through utilizing controls established internally.

Such areas may include working offices or meeting rooms where NATO Classified Information is stored, handled and/or discussed. These areas require:

- (i) a clearly defined and protected perimeter through which all entry and exit is controlled;
- (ii) an entry control system which permits unescorted access only to those individuals who are security cleared and authorised to enter the area; and
- (iii) an escort or equivalent control mechanism to deal with those individuals who do not meet the criteria described in sub-paragraph (b) (ii) above in order to prevent unauthorised access to NATO Classified Information and uncontrolled entry to areas which have been specifically designated as protected against technical attacks and eavesdropping.

Administrative Zone

11. An Administrative Zone shall be established around or leading to NATO Class I or Class II Security Areas. Only information classified NATO RESTRICTED (NR) may be stored, handled and/or discussed in Administrative Zones. Such areas require a visibly defined perimeter, within which the possibility exists for the control of individuals and vehicles. However, individuals are not required to be escorted.

Technically Secure Areas

12. Technically Secure Areas, either fixed or temporary, are areas which have been specifically identified as requiring protection against technical attacks and eavesdropping.

tekniska inspektioner, och tillträde till dem ska vara strikt kontrollerat. Följande åtgärder ska vidtas för att skydda utrymmena mot tekniska angrepp och avlyssning:

a) Adekvat nivå av fysiska och tekniska säkerhetsåtgärder för att i enlighet med risken verkställa behörighetskontroll. Ansvar för att fastställa risken delas mellan lämpliga tekniska sakkunniga och den säkerhetsmyndighet som ger råd till riskägaren i fråga om beslut eller godkännande.

b) Utrymmen av detta slag ska vara låsta och/eller bevakade när de inte används, och eventuella nycklar ska behandlas som säkerhetsnycklar. Regelbundna fysiska och/eller tekniska inspektioner ska utföras i enlighet med den behöriga säkerhetsmyndighetens krav. Inspektioner ska också utföras efter obehörigt tillträde eller misstanke om sådant samt efter att extern personal (till exempel för underhållsarbete eller ombyggnad) har haft tillträde till utrymmet.

c) Till dessa utrymmen får inga föremål, möbler och inventarier eller utrustning föras innan de har blivit noggrant undersökta av utbildad säkerhetspersonal med avseende på avlyssningsanordningar. En adekvat förteckning ska föras över föremål, möbler och inventarier och utrustning som flyttats till eller från dessa utrymmen.

d) I utrymmena får det inte finnas elektroniska system eller anordningar med in-splnings- och/eller sändningsfunktioner.

e) Telefoner och annan videokonferensutrustning får normalt inte installeras i dessa utrymmen. Om installation av sådana är oundviklig, ska de inte vara kopplade till nätet när säkerhetsskyddsklassificerade diskussioner förs i utrymmena. Detta gäller inte kommunikationsanordningar som är installerade och godkända på adekvat sätt.

Such areas shall be subject to regular physical and technical inspections and entry to them shall be strictly controlled. The following measures shall be applied to protect against technical attacks and eavesdropping:

(a) Appropriate level of physical and technical security measures to enforce access control, based upon the risk. The responsibility for determining the risk is shared between the appropriate technical specialists and the security authority which provides advice to the risk owner for a decision/approval.

(b) Such areas shall be locked and/or guarded when not occupied and any keys shall be treated as security keys. Regular physical and/or technical inspections, in accordance with the requirements of the appropriate security authority, shall be undertaken. Such inspections shall also be conducted following any unauthorised entry or suspicion thereof, as well as following the entry by external personnel (e.g. for the purposes of maintenance work, redecoration).

(c) No item, furnishing or equipment shall be allowed into these areas until they have been thoroughly examined for eavesdropping devices by trained security staff. An appropriate record of items, furnishing and equipment moved into and out of these areas shall be maintained.

(d) The presence of any electronic systems or devices with recording and/or transmitting capabilities shall be prohibited.

(e) Telephones and other video conference devices shall normally not be installed in such areas. However, where their installation is unavoidable, they shall be physically disconnected when classified discussions take place. This does not apply to appropriately installed and approved communication devices.

SÄRSKILDA FYSISKA SÄKERHETS-ÅTGÄRDER

13. Olika särskilda fysiska och tekniska säkerhetsåtgärder och säkerhetsförfaranden kan främja en organisations eller plats säkerhetsram. Dessa åtgärder och förfaranden omfattar bland annat yttre gränser, system för upptäckt av intrång, behörighetskontroll, övervakningskameror, säkerhetsbelysning, säkerhetsskåp och kontorsmöbler, lås, kontroll av nycklar och nummerkombinationer, besökarkontroll och kontroll vid in- och utpassering. Det stödjande direktivet om fysisk säkerhet innehåller närmare information om särskilda fysiska och tekniska säkerhetsåtgärder och säkerhetsförfaranden.

MINIMINORMER FÖR LAGRING AV NATOS SÄKERHETSSKYDDSKLASSIFICERADE INFORMATION

14. Natos säkerhetsskyddsklassificerade information ska lagras i utrymmen, säkerhetsskåp och/eller kontorsmöbler som är utformade för att avskräcka och upptäcka obehörig åtkomst till informationen.

15. **COSMIC TOP SECRET (CTS)**. Information som säkerhetsskyddsklassificerats som COSMIC TOP SECRET ska lagras i ett säkerhetsutrymme av klass I eller II i enlighet med något av följande villkor:

- a) i ett godkänt säkerhetsskåp och med en av följande kompletterande kontroller:
 - i) skyddas kontinuerligt av vid säkerhetsprövning godkänd vaktpersonal eller vakthavande personal,
 - ii) säkerhetsskåpet kontrolleras av vid säkerhetsprövning godkänd vaktpersonal eller vakthavande personal minst varannan timme vid slumpvisa tidpunkter, eller
 - iii) en kombination av ett godkänt system för upptäckt av intrång och en insatsstyrka som efter ett larm kommer till platsen inom den beräknade tidsram som behövs för att avlägsna eller bryta

SPECIFIC PHYSICAL SECURITY MEASURES

13. Various specific physical and technical security measures and procedures can contribute to the security framework of an organization or site. Such measures and procedures include but are not limited to: Perimeter, Intrusion Detection System (IDS), Access Control, Closed Circuit Television, Security Lighting, Secure Cabinets and Office Furniture, Locks, Control of Keys and Combinations, Visitor Control, Entry and Exit Searches. The supporting Directive on Physical Security provides detailed information on specific physical and technical security measures and procedures.

MINIMUM STANDARDS FOR STORAGE OF NATO CLASSIFIED INFORMATION

14. NATO Classified Information shall be stored in areas, secure cabinets and/or office furniture designed to deter and detect unauthorised access to the information.

15. **COSMIC TOP SECRET (CTS)**. Information classified CTS shall be stored within a Class I or Class II Security Area under one of the following conditions:

- (a) in an approved secure cabinet with one of the following supplemental controls:
 - (i) continuous protection by cleared guard or duty personnel;
 - (ii) inspection of the secure cabinet not less than every two hours, at randomly timed intervals, by cleared guard or duty personnel; or
 - (iii) an approved IDS in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe

upp säkerhetsskåpet eller för att övervinna de fysiska säkerhetsåtgärder som används,

b) i ett öppet lagringsutrymme som är konstruerat i enlighet med kraven i det stödjande direktivet om fysisk säkerhet och som är utrustat med ett system för upptäckt av intrång i kombination med en insatsstyrka som efter ett larm kommer till platsen inom den beräknade tidsram som behövs för intrång genom tvång, eller

c) i ett valv med ett system för upptäckt av intrång i kombination med en insatsstyrka som efter ett larm kommer till platsen inom den beräknade tidsram som behövs för intrång genom tvång.

16. NATO SECRET (NS). Information som säkerhetsskyddsklassificerats som NATO SECRET ska lagras i ett säkerhetsutrymme av klass I eller II på något av följande sätt:

a) så som föreskrivs för information som säkerhetsskyddsklassificerats som COSMIC TOP SECRET,

b) i ett godkänt säkerhetsskåp eller valv utan kompletterande kontroller, eller

c) i ett öppet lagringsutrymme, varvid åtminstone en av följande kompletterande kontroller krävs:

i) den plats där det öppna lagringsutrymmet finns ska kontinuerligt skyddas av vid säkerhetsprövning godkänd vaktpersonal eller vakthavandepersonal,

ii) det öppna lagringsutrymmet ska kontrolleras av vid säkerhetsprövning godkänd vaktpersonal eller vakthavande personal minst en gång var fjärde timme, eller

iii) ett system för upptäckt av intrång i kombination med en insatsstyrka som efter ett larm kommer till platsen inom den beräknade tidsram som behövs för intrång genom tvång.

17. NATO CONFIDENTIAL (NC). Information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL ska lagras i

needed to remove or break open the secure cabinet, or overcome the physical security measures in place;

(b) in an open storage area constructed in accordance with the requirements set out in the supporting Directive on Physical Security, which is equipped with an IDS in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed for forced entry; or

(c) in an IDS-equipped vault in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed for forced entry.

16. NATO SECRET (NS). Information classified NS shall be stored within a Class I or Class II Security Area by one of the following methods:

(a) in the same manner as prescribed for information classified CTS;

(b) in an approved secure cabinet or vault without supplemental controls; or

(c) in an open storage area, in which case one of the following supplemental controls is required:

(i) the location that houses the open storage area shall be subject to continuous protection by cleared guard or duty personnel;

(ii) cleared guard or duty personnel shall inspect the open storage area not less than once every four hours; or

(iii) an IDS in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed for forced entry.

17. NATO CONFIDENTIAL (NC). Information classified NC shall be stored in a

ett godkänt säkerhetsskåp i ett säkerhetsutrymme av klass I eller II.

18. **NATO RESTRICTED (NR).** Information som säkerhetsskyddsklassificerats som NATO RESTRICTED ska lagras i ett låst skåp eller en låst kontorsmöbel (till exempel skrivbordslåda) i en administrativ zon, ett säkerhetsutrymme av klass I eller ett säkerhetsutrymme av klass II. Information som säkerhetsskyddsklassificerats som NATO RESTRICTED får också lagras i ett låst skåp, valv eller öppet lagringsutrymme som är godkänt för information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller högre.

19. Ytterligare detaljer och krav i fråga om lagring av Natos säkerhetsskyddsklassificerade information finns i det stödjande direktivet om fysisk säkerhet.

FYSISKT SKYDD FÖR KOMMUNIKATIONS- OCH INFORMATIONSSYSTEM

20. Utrymmen där Natos säkerhetsskyddsklassificerade information presenteras eller hanteras med hjälp av informationsteknik eller där det är möjligt att få åtkomst till sådan information ska inrättas på ett sådant sätt att det övergripande kravet på konfidentialitet, riktighet och tillgänglighet uppfylls.

21. Utrymmen där kommunikations- och informationssystem används för att visa, lagra, bearbeta eller överföra information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller högre eller där det är möjligt att få åtkomst till sådan information, ska inrättas som säkerhetsutrymmen av Natos klass I eller II eller motsvarande nationella säkerhetsutrymmen. Utrymmen där kommunikations- och informationssystem används för att visa, lagra, bearbeta eller överföra information som säkerhetsskyddsklassificerats som NATO RESTRICTED eller där det är möjligt att få åtkomst till sådan information får inrättas som administrativa zoner.

Class I or Class II Security Area in an approved secure cabinet.

18. **NATO RESTRICTED (NR).** Information classified NR shall be stored in a locked cabinet or office furniture (e.g. office desk drawer) within an Administrative Zone, Class I Security Area, or Class II Security Area. Information classified NR may also be stored in a locked cabinet, vault, or open storage area approved for information classified NC or higher.

19. Additional details and requirements for the storage of NATO Classified Information are set out in the supporting Directive on Physical Security.

PHYSICAL PROTECTION OF COMMUNICATION AND INFORMATION SYSTEMS

20. Areas in which NATO Classified Information is presented or handled using information technology, or where potential access to such information is possible, shall be established in a way that the aggregate requirement for confidentiality, integrity and availability is met.

21. Areas in which CIS are used to display, store, process, or transmit information classified NC and above, or where potential access to such information is possible, shall be established as NATO Class I or Class II Security Areas or the national equivalent. Areas in which CIS are used to display, store, process or transmit information classified NR, or where potential access to such information is possible, may be established as Administrative Zones.

22. Tillträde till utrymmen där ytterst viktiga komponenter i kommunikations- och informationssystem förvaras och hanteras ska särskilt kontrolleras och begränsas till endast personal med tillstånd att vara i utrymme och anknäring till säkerhet och system-/nät-/krypteringsadministrering.

SKYDD MOT TEKNISKA ANGREPP

23. Kontor eller utrymmen där information som säkerhetsskyddsklassificerats som NATO SECRET regelbundet diskuteras ska med hjälp av pålitliga fysiska säkerhetsåtgärder och behörighetskontroll skyddas mot passiva och aktiva avlyssningsangrepp, om risken förutsätter det. Ansvar för att fastställa risken ska samordnas med tekniska sakkunniga, och beslut om det ska fattas av en behörig säkerhetsmyndighet. Det stödande direktivet om fysisk säkerhet innehåller närmare information om skydd mot passiv och aktiv avlyssning.

GODKÄND UTRUSTNING

24. Natos medlemsstater får endast använda utrustning som har godkänts för skydd av Natos säkerhetsskyddsklassificerade information av behörig säkerhetsmyndighet. Natos civila och militära organ ska se till att all utrustning som köpts har godkänts av en av Natos medlemsstater för användning i liknande förhållanden. Natos civila och militära organ får också köpa utrustning som blivit godkänd för användning av en behörig säkerhetsmyndighet på grundval av en slutförd riskbedömning som stöder minskning eller begränsning av den identifierade risken eller de identifierade riskerna.

22. Access to areas where critical CIS components are housed and managed shall be specifically controlled and limited to only authorised personnel associated with security and system/network/crypto administration.

PROTECTION AGAINST TECHNICAL ATTACKS

23. Offices or areas in which information classified NS and above is regularly discussed shall be protected against passive and active eavesdropping attacks, by means of sound physical security measures and access control, where the risk warrants it. The responsibility for determining the risk shall be co-ordinated with technical specialists and decided by the appropriate security authority. The supporting Directive on Physical Security provides details on protection against passive and active eavesdropping.

APPROVED EQUIPMENT

24. NATO Nations shall only use equipment which has been approved for the protection of NATO Classified Information by an appropriate security authority. NATO Civil and Military bodies shall ensure that any equipment purchased has been approved for use by one of the NATO Nations in similar conditions. NATO Civil and Military bodies may also purchase equipment approved for use by an appropriate security authority based on a completed risk assessment that supports the reduction or mitigation of the identified risk(s).

BILAGA E
C-M(2002)49-REV1

ENCLOSURE "E"
C-M(2002)49-REV1

**BILAGA E
SÄKERHET FÖR NATOS SÄKERHETSSKYDDSKLASSIFICERADE INFORMATION**

**ENCLOSURE "E"
SECURITY OF NATO CLASSIFIED INFORMATION**

INLEDNING

1. I denna bilaga presenteras strategin och miniminormerna för säkerheten för Natos säkerhetsskyddsklassificerade information. Ytterligare detaljer och krav finns i det stödande direktivet om säkerhet för Natos säkerhetsskyddsklassificerade information (AC/35-D/2002).

2. Informationssäkerhet är vidtagande av allmänna skyddsåtgärder och tillämpning av skyddsförfaranden för att förhindra, upptäcka och avhjälpa förlust eller läcka av säkerhetsskyddsklassificerad information. Säkerhetsskyddsklassificerad information ska skyddas under hela sin livscykel i enlighet med en nivå som motsvarar dess säkerhetsskyddsklassificering. Vid hanteringen ska det ses till att den har en lämplig säkerhetsskyddsklassificering, är tydligt identifierad som säkerhetsskyddsklassificerad information och förblir säkerhetsskyddsklassificerad endast så länge som detta behövs. Informationssäkerhet ska kompletteras med personalsäkerhet, fysisk säkerhet och säkerhet i kommunikations- och informationssystem för att säkerställa en balanserad uppsättning åtgärder som skydd för Natos säkerhetsskyddsklassificerade information.

NATOS SÄKERHETSSKYDDSKLASSIFICERING, SÄRSKILDA KODER, MÄRKNINGAR OCH ALLMÄNNA PRINCIPER

3. Den som informationen härrör från ansvarar för att fastställa säkerhetsskyddsklassificeringen och den första spridningen av den säkerhetsskyddsklassificerade informationen.

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for the security of NATO Classified Information. Additional details and requirements are found in the supporting Directive on the Security of NATO Classified Information (AC/35-D/2002).

2. Security of information is the application of general protective measures and procedures to prevent, detect and recover from the loss or compromise of classified information. Classified information shall be protected throughout its life cycle to a level commensurate with its security classification. It shall be managed to ensure that it is appropriately classified, is clearly identified as classified and remains classified only as long as this is necessary. Security of information shall be complemented by Personnel, Physical and Communication and Information Systems (CIS) Security in order to ensure a balanced set of measures for the protection of NATO Classified Information.

NATO SECURITY CLASSIFICATIONS, SPECIAL DESIGNATORS, MARKINGS AND GENERAL PRINCIPLES

3. The originator is responsible for determining the security classification and initial dissemination of classified information.

4. Säkerhetsskyddsklassificeringsnivån får inte ändras eller sänkas och beslut om att informationen inte längre ska vara säkerhetsskyddsklassificerad får inte fattas utan samtycke av den som informationen härrör från. När säkerhetsskyddsklassificeringsnivån fastställs ska den som informationen härrör från om möjligt ange huruvida den säkerhetsskyddsklassificerade informationen kan inplaceras på en lägre säkerhetsskyddsklassificeringsnivå eller beslut om att informationen inte längre ska vara säkerhetsskyddsklassificerad kan meddelas vid en viss tidpunkt eller händelse.

5. Den angivna säkerhetsskyddsklassificeringen avgör med hurdan fysisk säkerhet och säkerhet i kommunikations- och informationssystem informationen skyddas när den lagras, överförs, sänds, sprids och utplånas samt en hurdan godkänd säkerhetsprövning av person (PSC) som krävs för åtkomst till informationen. Därför ska både överklassificering och underklassificering undvikas för att garantera faktisk säkerhet och effektivitet.

6. Säkerhetsskyddsklassificerad information ska föras med märkning av säkerhetsskyddsklassificering för att ange vilken eventuell skada Natos och/eller dess medlemsstaters säkerhet kan drabbas av om informationen är föremål för obehörigt röjande. Den som den säkerhetsskyddsklassificerade informationen härrör från har privilegiet att fastställa eller ändra säkerhetsskyddsklassificeringen. Natos säkerhetsskyddsklassificeringsnivåer och deras betydelse är följande:

- a) COSMIC TOP SECRET (CTS)
obehörigt röjande skulle orsaka Nato exceptionellt allvarlig skada,
- b) NATO SECRET (NS)
obehörigt röjande skulle orsaka Nato allvarlig skada,
- c) NATO CONFIDENTIAL (NC)
obehörigt röjande skulle skada Nato, och
- d) NATO RESTRICTED (NR)

4. The security classification shall not be changed, downgraded or declassified without the consent of the originator. At the time of its creation, the originator shall indicate, where possible, whether their classified information can be downgraded or declassified on a certain date or event.

5. The security classification assigned determines the physical and CIS Security provided to the information in storage, transfer and transmission, its circulation, destruction and the Personnel Security Clearance (PSC) required for access. Therefore, both overclassification and underclassification shall be avoided in the interests of effective security as well as efficiency.

6. Security classifications shall be applied to classified Information in order to indicate the possible damage to the security of NATO and/or its member Nations if the information is subjected to unauthorised disclosure. It is the prerogative of the originator of the classified information to determine or modify the security classification. NATO security classifications and their significance are:

- (a) COSMIC TOP SECRET (CTS)
unauthorised disclosure would result in exceptionally grave damage to NATO;
- (b) NATO SECRET (NS)
unauthorised disclosure would result in grave damage to NATO;
- (c) NATO CONFIDENTIAL (NC)
unauthorised disclosure would be damaging to NATO; and
- (d) NATO RESTRICTED (NR)

obehörigt röjande skulle vara icke önskvärdt för Natos intressen och effektivitet.

7. Natos säkerhetsskyddsklassificering visar hur känslig Natos säkerhetsskyddsklassificerade information är och tillämpas för att fästa mottagarnas uppmärksamhet vid behovet av att säkerställa ett skydd som motsvarar den grad av skada som skulle uppstå till följd av obehörig åtkomst eller obehörigt röjande.

8. Den information som säkerhetsskyddsklassificerats som NATO UNCLASSIFIED eller offentlig information ska skyddas och hanteras i enlighet med strategin för hantering av Natinformation (C-M(2007)0118) och handlingen om hanteringen av icke-säkerhetsskyddsklassificerad Natinformation (C-M(2002)60).

9. Planeringen, förberedelserna, genomförandet och stödet i samband med Natos operationer, utbildning, övningar, transformation och samarbete (OTETC) kan kräva att särskilda ytterligare säkerhetsaspekter beaktas; den stödjande handlingen om delning av underrättelseinformation och annan information med enheter som inte hör till Nato (AC/35-D/1040) innehåller säkerhetsbestämmelser och säkerhetsanvisningar som är tillämpliga i dessa situationer.

10. Natos medlemsstater och Natos civila och militära organ ska vidta åtgärder i syfte att se till att säkerhetsskyddsklassificerad information som skapats av eller tillhandahållits Nato ges korrekt säkerhetsskyddsklassificering och skyddas i enlighet med kraven i det stödjande direktivet om säkerhet för Natos säkerhetsskyddsklassificerade information.

11. Vart och ett av Natos civila eller militära organ ska inrätta ett system för säkerställande av att information som säkerhetsskyddsklassificerats som COSMIC TOP SECRET och som härrör från organet ses över minst vart femte år och information som säkerhetsskyddsklassificerats som NATO SECRET ses över minst vart tionde

unauthorised disclosure would be detrimental to the interests or effectiveness of NATO.

7. NATO security classifications indicate the sensitivity of NATO Classified Information and are applied in order to alert recipients to the need to ensure protection in proportion to the degree of damage that would occur from unauthorised access or disclosure.

8. NATO UNCLASSIFIED information and Information releasable to the Public shall be protected and handled in accordance with the NATO Information Management Policy (C-M(2007)0118) and The Management of Non-Classified NATO Information (C-M(2002)60).

9. The planning, preparation, execution and support relating to NATO Operations, Training, Exercises, Transformation and Cooperation (OTETC) may require specific additional security aspects to be addressed; the Supporting Document on Information and Intelligence Sharing with Non-NATO Entities (AC/35-D/1040) contains security provisions and guidance applicable in these circumstances.

10. NATO Nations and NATO Civil and Military bodies shall introduce measures to ensure that classified information created by, or provided to NATO is assigned the correct security classification, and is protected in accordance with the requirements of the supporting Directive on the Security of NATO Classified Information.

11. Each NATO Civil or Military Body shall establish a system to ensure that CTS information which it has originated is reviewed no less frequently than every five years and NS information no less frequently than every 10 years in order to ascertain whether the security classification still applies. Such

är för att kontrollera om säkerhetsskyddsklassificeringen fortfarande är tillämplig. En sådan översyn är inte nödvändig i de fall där den som informationen härrör från i förväg har bestämt att särskild säkerhetsskyddsklassificerad Natoinformation automatiskt ska inplaceras på en lägre säkerhetsskyddsklassificeringsnivå efter en i förväg bestämd period och informationen har märkts på detta sätt.

12. Den övergripande säkerhetsskyddsklassificeringen för en handling ska vara minst lika hög som den del som fått den högsta säkerhetsskyddsklassificeringen. Omslag ska märkas med Natos säkerhetsskyddsklassificering som tillämpas på hela den information som de bifogats till. Om möjligt ska till exempel stycken, bilagor, tillägg och så vidare i handlingar som säkerhetsskyddsklassificerats som NATO RESTRICTED eller högre märkas på lämpligt sätt av den som informationen härrör från för att underlätta beslut om ytterligare spridning.

13. När en stor mängd av Natos säkerhetsskyddsklassificerade information samlas ihop ska de ursprungliga säkerhetsskyddsklassificeringsmärkningarna bibehållas och en bedömning av hur organisationen påverkas om den samlade informationen går förlorad eller läcker göras. Om denna övergripande effekt bedöms vara större än effekten av Natos berörda enskilda säkerhetsskyddsklassificeringsnivåer, ska hantering och skydd av den samlade informationen på en nivå som motsvarar den bedömda effekten av att den samlade informationen går förlorad eller läcker övervägas.

Ytterligare märkningar

14. COSMIC och NATO är märkningar som när de tillämpas på Natos säkerhetsskyddsklassificerade information innebär att informationen ska skyddas i enlighet med Natos säkerhetsstrategi.

Beteckningar för särskilda kategorier

15. ATOMAL är en märkning som används på information av särskild kategori och som

a review is not necessary in those instances where the originator has predetermined that specific NATO Classified Information shall be automatically downgraded after a predetermined period and the classified information has been so marked.

12. The overall security classification of a document shall be at least as high as that of its most highly classified component. Covering documents shall be marked with the overall NATO security classification of the information to which they are attached. Where possible, component parts like paragraphs, enclosures, annexes, etc., of documents classified NR and above should be marked appropriately by the originator to facilitate decisions on further dissemination.

13. When a large amount of NATO Classified Information is collated together, the original security classification markings shall be retained and that information shall be assessed for the impact its collective loss or compromise would have upon the organization. If this overall impact is assessed as being higher than the impact of the actual individual NATO security classifications then consideration should be given to handling and protecting it at a level commensurate with the assessed impact of its loss or compromise.

Qualifying Markings

14. The terms COSMIC and NATO are qualifying markings which, when applied to NATO Classified Information, signify that the information shall be protected in accordance with NATO Security Policy.

Special Category Designators

15. The term "ATOMAL" is a marking applied to special category information signifying that the information shall be protected

anger att informationen ska skyddas i enlighet med avtalet mellan parterna i nordatlantiska fördraget om samarbete avseende nukleär information (C-M(64)39) och de stödjande administrativa arrangemangen (C-M(68)41).

16. SIOP är en märkning som används på information av särskild kategori och som anger att informationen ska skyddas i enlighet med C-M(71)27(Reviderad), som gäller särskilda förfaranden för hantering av information om Förenta staternas gemensamma operativa plan (US-Siop) i Nato.

17. CRYPTO är en märkning och en särskild kategoribeteckning som anges på allt Comsec-nyckelmateriel som används för att skydda eller autentisera telekommunikation som innehåller Natos kryptografiska säkerhetsrelaterad information och som anger att informationen ska skyddas i enlighet med lämpliga kryptografiska säkerhetsstrategier och säkerhetsdirektiv.

18. BOHEMIA är en märkning som används för information av särskild kategori som härrör från eller avser kommunikationssignalspaning (COMINT). All information med märkningen COSMIC TOP SECRET — BOHEMIA skyddas strikt i enlighet med MC 101 (Natos signalspaningsstrategi) och alliansens gemensamma publikation AJP, som redogör för MC 101 och som berör tillämpliga principer, samt den handbok om Sigint-administrationen och Sigint-förfarandena som Natos rådgivande kommitté för signalspaning publicerat.

Märkningar om begränsad spridning

19. Den som informationen härrör från kan använda en märkning om begränsad spridning som en ytterligare märkning genom vilken spridningen av Natos säkerhetsskyddsklassificerade information begränsas ytterligare.

KONTROLL OCH HANTERING

Syftena med ansvarsskyldighet

in accordance with the Agreement between the Parties to the North Atlantic Treaty for Co-operation Regarding Atomic Information (C-M(64)39) and the supporting Administrative Arrangements (C-M(68)41).

16. The term "SIOP" is a marking applied to special category information signifying that the information shall be protected in accordance with "Special Procedures for the Handling of United States Single Integrated Operational Plan (US-SIOP) Information Within NATO C-M(71)27(Revised)".

17. The term "CRYPTO" is a marking and a special category designator identifying all COMSEC keying material used to protect or authenticate telecommunications carrying NATO cryptographic security-related information; signifying that the information shall be protected in accordance with the appropriate cryptographic security policies and directives.

18. The term "BOHEMIA" is a marking applied to special category information derived from or pertaining to Communications Intelligence (COMINT). All information marked COSMIC TOP SECRET - BOHEMIA will be protected in strict accordance with MC 101 (NATO Signals Intelligence Policy) and its companion Allied Joint Publication (AJP) which covers doctrine and the NACSI Guide to SIGINT Administration and Procedures which addresses administration and procedures.

Dissemination Limitation Markings

19. As an additional marking to further limit the dissemination of NATO Classified Information, a Dissemination Limitation Marking may be applied by the originator.

CONTROL AND HANDLING

Objectives of Accountability

20. Huvudsyftet med ansvarsskyldigheten är att tillhandahålla tillräcklig information för undersökning av en avsiktlig eller oavsiktlig förlust eller läcka av information som omfattas av ansvarsskyldighet och att bedöma de skador som uppstått till följd av förlusten eller läckan. Kravet på ansvarsskyldighet syftar till att skapa disciplinerad hantering och kontroll av åtkomst till information som omfattas av ansvarsskyldighet.

21. De underordnade målen är

- a) att följa åtkomsten till information som omfattas av ansvarsskyldighet, det vill säga vem som faktiskt eller potentiellt har haft åtkomst till informationen och vem som har försökt få åtkomst till informationen,
- b) att känna till var information som omfattas av ansvarsskyldighet finns,
- c) att följa var information som omfattas av ansvarsskyldighet rör sig inom Nato och nationellt, och
- d) att föra bok över information som omfattas av ansvarsskyldighet och som har lämnats ut till enheter som inte hör till Nato.

22. Information som säkerhetsskyddsklassificerats som COSMIC TOP SECRET, NATO SECRET eller ATOMAL ska omfattas av ansvarsskyldighet samt kontrolleras och hanteras i enlighet med kraven i denna bilaga och det stödjande direktivet om säkerhet för Natos säkerhetsskyddsklassificerade information. Om så krävs enligt nationella lagar och regler, kan den information som är försedd med någon annan säkerhetsskyddsklassificering eller särskild kategorimärkning betraktas som information som omfattas av ansvarsskyldighet.

Registreringssystemet

23. Registreringssystemets säkerhetsförfaranden och säkerhetskrav gäller på samma sätt i både fysiska och elektroniska miljöer. Ytterligare detaljer och krav som gäller de elektroniska miljöerna finns i bilaga F till

20. The primary objective of accountability is to provide sufficient information to be able to investigate a deliberate or accidental loss or compromise of accountable information and assess the damage arising from the loss or compromise. The requirement for accountability serves to impose a discipline on the handling of, and control of access to, accountable information.

21. Subordinate objectives are:

- (a) to keep track of access to accountable information – who has, or potentially has, had access to accountable information; and who has attempted to access accountable information;
- (b) to know the location of accountable information;
- (c) to keep track of the movement of accountable information within the NATO and national domains; and
- (d) register accountable information that has been released to NNEs.

22. Information classified CTS, NS and ATOMAL shall be accountable, controlled and handled in accordance with the requirements of this Enclosure and the supporting Directive on the Security of NATO Classified Information. Where required by national laws and regulations, information bearing other classification or special category markings may be considered as accountable information.

The Registry System

23. The security procedures and requirements of the registry system apply equally across both the physical and electronic domains. Additional details and requirements concerning the electronic domain can be

denna C-M-handling och i handlingens stöd-
jande direktiv.

24. Det ska finnas ett registreringssystem med ansvar för mottagande, registrering, hantering, distribution och utplåning av information som omfattas av ansvarsskyldighet. Detta ansvar kan fullgöras antingen genom ett enda registreringssystem, varvid information som säkerhetsskyddsklassificerats som COSMIC TOP SECRET och annan information av särskild kategori alltid ska vara strikt åtskilda, eller genom att inrätta separata register och kontrollpunkter.

25. Beroende på vad som är lämpligt ska varje medlemsstat i Nato eller vart och ett av Natos civila eller militära organ inrätta ett eller flera centralregister för information som säkerhetsskyddsklassificerats som COSMIC TOP SECRET, varvid registret fungerar som den huvudsakliga mottagande och avsändande myndigheten i den medlemsstat eller det organ där det har inrättats. Centralregistret kan också fungera som ett register för annan information som omfattas av ansvarsskyldighet.

26. Registren och kontrollpunkterna ska fungera som ansvariga organisationer för den interna distributionen av information som säkerhetsskyddsklassificerats som COSMIC TOP SECRET och NATO SECRET och för registreringen av all information som omfattas av ansvarsskyldighet och som registret eller kontrollpunkten i fråga ansvarar för; registren och kontrollpunkterna kan inrättas på ministerie-, avdelnings- eller ledningsnivå. Information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller NATO RESTRICTED behöver inte registreras i registreringssystemet, om inte det föreskrivs i nationella lagar och regler.

27. Register och kontrollpunkter ska alltid kunna lokalisera var Natoinformation som omfattas av ansvarsskyldighet finns. Oregelbunden och tillfällig åtkomst till sådan information kräver inte nödvändigtvis att ett register eller en kontrollpunkt inrättas, förut-

found within Enclosure "F" to this C-M and its supporting directives.

24. There shall be a Registry System which is responsible for the receipt, accounting, handling, distribution and destruction of accountable information. Such a responsibility may be fulfilled either within a single Registry System, in which case strict compartmentalisation of information classified CTS and other special category information shall be maintained at all times, or by establishing separate registries and control points.

25. Each NATO Nation or NATO Civil or Military Body, as appropriate, shall establish a Central Registry(s) for information classified CTS, which acts as the main receiving and dispatching authority for the Nation or body within which it has been established. The Central Registry(s) may also act as a registry(s) for other accountable information.

26. Registries and control points shall act as the responsible organization for the internal distribution of information classified CTS and NS and for keeping records of all accountable information held on that registry's or control point's charge; they may be established at ministry, department, or command levels. NC and NR information is not required to be processed through the Registry System unless specified by national laws and regulations.

27. With regard to NATO accountable information, registries and control points shall be able at all times to establish its location. Infrequent and temporary access to such information does not necessarily require the establishment of a registry or control point,

satt att det finns förfaranden för säkerställande av att informationen förblir under registreringssystemets kontroll.

28. Spridningen av information som säkerhetsskyddsklassificerats som COSMIC TOP SECRET ska ske via Cosmic-registret. I varje register ska minst en gång per år en inventering av all information som omfattas av ansvarsskyldighet som säkerhetsskyddsklassificerats som COSMIC TOP SECRET göras i enlighet med kraven i det stödjande direktivet om säkerhet för Natos säkerhetsskyddsklassificerade information. Oberoende av typen av registerorganisation ska de organisationer som hanterar information som säkerhetsskyddsklassificerats som COSMIC TOP SECRET utse en Cosmic-tjänsteman med ansvar för kontroll (CCO).

29. I det stödjande direktivet om säkerhet för Natos säkerhetsskyddsklassificerade information fastställs bland annat vad Cosmic-tjänstemannen med ansvar för kontroll ansvarar för, detaljerade förfaranden för hantering av information som säkerhetsskyddsklassificerats som COSMIC TOP SECRET eller NATO SECRET i registreringssystemet, förfaranden för återgivning och överlämning av samt utdrag ur Natos säkerhetsskyddsklassificerade information, krav för spridning och överföring av den samt krav för eliminering och utplåning av den.

30. Militärkommittén har inrättat ett separat system för fullgörande av ansvarsskyldighet samt för kontroll och distribution när det gäller kryptografiskt material. Material som överförs genom detta system kräver inte fullgörande av ansvarsskyldighet i registreringssystemet.

BEREDSKAPSPLANERING

31. Natos medlemsstater och Natos civila och militära organ ska utarbeta beredskapsplaner för skydd eller utplåning av Natos säkerhetsskyddsklassificerade information i krislägen för att förhindra obehörig åtkomst

provided that procedures are in place to ensure that the information remains under the control of the Registry System.

28. The dissemination of information classified CTS shall be through COSMIC registry channels. At least annually, each registry shall carry out an inventory of all information classified CTS for which it is accountable, in accordance with the requirements of the supporting Directive on the Security of NATO Classified Information. Regardless of the type of registry organization, those that handle information classified CTS shall appoint a "COSMIC Control Officer" (CCO).

29. The supporting Directive on the Security of NATO Classified Information sets out, inter alia, the responsibilities of the CCO, the detailed registry system handling processes for information classified CTS and NS, the procedures for reproductions, translations and extracts, the requirements for the dissemination and transfer, and the requirements for the disposal and destruction of NATO Classified Information.

30. The Military Committee (MC) has established a separate system for the accountability, control and distribution of cryptographic material. Material being transferred through this system does not require accountability in the Registry System.

CONTINGENCY PLANNING

31. NATO Nations and NATO Civil and Military bodies shall prepare contingency plans for the protection or destruction, during emergency situations, of NATO Classified Information to prevent unauthorised access and disclosure and loss of availability.

eller obehörigt röjande, eller att tillgänglighet går förlorad. Dessa planer ska grunda sig på regelbundet granskade hotbedömningar och ge högsta prioritet åt den känsligaste informationen och den uppdrags- och tidskritiska informationen.

SÄKERHETSINCIDENTER

32. En säkerhetsincident är en händelse eller någon annan tilldragelse som kan ha en negativ inverkan på säkerheten för Natos säkerhetsskyddsklassificerade information och som kräver ytterligare utredningsåtgärder för exakt avgörande av om den utgör en säkerhetsöverträdelse eller säkerhetsförseelse.

Säkerhetsöverträdelse

33. En säkerhetsöverträdelse är en avsiktlig eller oavsiktlig handling eller underlåtenhet som strider mot säkerhetsbestämmelserna i denna strategi och som kan leda till en faktisk eller eventuell läcka av Natos säkerhetsskyddsklassificerade information eller de stödjande tjänsterna och resurserna.

Läcka

34. En läcka innebär en situation där Natos säkerhetsskyddsklassificerade information eller de stödjande tjänsterna och resurserna på grund av en säkerhetsöverträdelse eller på grund av skadlig verksamhet har förlorat sin konfidentialitet, riktighet eller tillgänglighet. Detta innebär förlust, röjande till obehöriga personer, otillåtna ändringar, utplåning på otillåtet sätt eller överbelastning.

Förseelse

35. En förseelse är en avsiktlig eller oavsiktlig handling eller underlåtenhet som strider mot säkerhetsbestämmelserna i denna strategi och som inte leder till en faktisk eller eventuell läcka av Natos säkerhetsskyddsklassificerade information.

36. Alla säkerhetsöverträdelser eller eventuella säkerhetsöverträdelser ska omedelbart rapporteras till den behöriga säkerhetsmyndigheten. Varje rapporterad säkerhetsöver-

These plans will be based on periodically reviewed threat assessments and shall give highest priority to the most sensitive, and mission- or time-critical information.

SECURITY INCIDENTS

32. A Security Incident is an event or other occurrence that may have an adverse effect upon the security of NATO Classified Information which requires further investigative actions in order to accurately determine whether or not it constitutes a Security Breach or Infraction.

Security Breach

33. A Security Breach is an act or omission, deliberate or accidental, contrary to the security rules laid down in this policy that may result in the actual or possible compromise of NATO Classified Information or supporting services and resources.

Compromise

34. Compromise denotes a situation when, due to a Security Breach or adverse activity, NATO Classified Information has lost its confidentiality, integrity or availability, or supporting services and resources have lost their integrity or availability. This includes loss, disclosure to unauthorized individuals, unauthorised modification, destruction in an unauthorised manner, or denial of service.

Infraction

35. Infraction is an act or omission, deliberate or accidental, contrary to the security rules laid down in this policy, that does not result in the actual or possible compromise of NATO Classified Information.

36. All Security Breaches or potential Security Breaches shall be reported immediately to the appropriate security authority. Each reported Security Breach shall be investi-

trädelse ska utredas av personer som har erfarenhet av säkerhet, utredning och, i förekommande fall, kontrapionage och som är oberoende av de personer som direkt berörs av säkerhetsöverträdelsen. Det stödjande direktivet om säkerhet för Natos säkerhetskyddsklassificerade information innehåller närmare information om de åtgärder som ska vidtas vid upptäckt av en säkerhetsöverträdelse eller säkerhetsförseelse.

RAPPORTERING

37. Huvudsyftet med att rapportera säkerhetsöverträdelser och läckor av Natos säkerhetskyddsklassificerade information är att ge den Natoaktör som informationen härrör från möjlighet att bedöma den skada som Nato åsamkas och att vidta behövliga eller möjliga åtgärder för att minimera skadan. Rapporter om skadebedömningen och de minimeringsåtgärder som vidtagits ska sändas till Natos säkerhetsbyrå av den nationella säkerhetsmyndigheten eller den utsedda säkerhetsmyndigheten eller av chefen för det berörda civila eller militära Natoorganet.

38. Om möjligt ska den Natoaktör som informationen härrör från informeras samtidigt som Natos säkerhetsbyrå av den rapporterande myndigheten, men Natos säkerhetsbyrå kan uppmanas att informera när den som informationen härrör från är svår att identifiera. Tidpunkten för att lämna in rapporter till Natos säkerhetsbyrå beror på informationens känslighet och omständigheterna.

39. Natos säkerhetsbyrå kan på Natos generalsekreterares vägnar begära att de behöriga myndigheterna gör ytterligare utredningar och rapporterar sina upptäckter till Natos säkerhetsbyrå. Beroende på omständigheterna och hur allvarlig läckan är kan Natos säkerhetsbyrå informera säkerhetskommittén.

40. I det stödjande direktivet om säkerhet för Natos säkerhetskyddsklassificerade information fastställs i detalj åtgärder, registrering och rapporteringskrav vid säkerhetsöverträdelser och äventyrande av säkerheten.

gated by individuals who have security, investigative and, where appropriate, counterintelligence experience, and who are independent of those individuals immediately concerned with the Security Breach. The supporting Directive on Security of NATO Classified Information provides details on actions to be taken upon discovery of a Security Breach or Infraction.

REPORTING

37. The main purpose of reporting Security Breaches and compromises of NATO Classified Information is to enable the originating NATO component to assess the resulting damage to NATO and to take whatever action is desirable or practicable to minimize the damage. Reports of the damage assessment and minimising action taken shall be forwarded to the NOS by the NSA/DSA or Head of the NATO Civil or Military Body concerned.

38. Where possible, the reporting authority should inform the originating NATO component at the same time as the NOS, but the latter may be requested to do this when the originator is difficult to identify. The timing of submitting reports to the NOS depends on the sensitivity of the information and the circumstances.

39. The NOS, on behalf of the Secretary General of NATO, may request the appropriate authorities to make further investigations and to report their findings back to the NOS. Depending upon the circumstances and severity of the compromise, the NOS may inform the Security Committee (SC).

40. The supporting Directive on the Security of NATO Classified Information sets out the detailed actions, records and reporting requirements for Security Breaches and compromises of security.

41. Särskilda bestämmelser om läckor av kryptografiskt material har utfärdats av militärkommittén till kommunikationssäkerhetsmyndigheterna i Natos medlemsstater och till Natos civila och militära organ.

41. Separate provisions relating to the compromise of cryptographic material have been issued by the MC to communications security authorities of NATO Nations and NATO Civil and Military bodies.

BILAGA F
C-M(2002)49-REV1

ENCLOSURE "F"
C-M(2002)49-REV1

**BILAGA F
SÄKERHET I KOMMUNIKATIONS-
OCH INFORMATIONSSYSTEM**

**ENCLOSURE "F"
COMMUNICATION AND INFOR-
MATION SYSTEM SECURITY**

1. INLEDNING

1.1. I denna bilaga presenteras strategin och miniminormerna för skydd av Natos säkerhetsskyddsklassificerade information och systemstödjande tjänster och resurser¹ när det gäller kommunikations- och informationssystem och andra elektroniska system vid lagring, bearbetning eller överföring av Natos säkerhetsskyddsklassificerade information.

1.2. Denna bilaga stöder Natos strategi för informationshantering och kompletterar strategin för hantering av icke-säkerhetsskyddsklassificerad Natoinformation där de grundläggande principer och normer finns som ska tillämpas i Natos civila och militära organ samt Natos medlemsstater för att skydda icke-säkerhetsskyddsklassificerad Natoinformation.

1.3. Säkerhet i kommunikations- och informationssystem (CIS Security) är en av faktorerna vid informationssäkring (figur 1) och definieras som vidtagande av säkerhetsåtgärder för att skydda kommunikations- och informationssystem och andra elektroniska system² samt den information som lagras, behandlas eller överförs³ i dessa system med avseende på konfidentialitet, riktighet, tillgänglighet, autentisering och oavvislighet.

1. INTRODUCTION

1.1. This Enclosure sets out the policy and minimum standards for the protection of NATO classified information, and supporting system services and resources¹ in communication, information and other electronic systems storing, processing or transmitting NATO classified information.

1.2. This Enclosure supports the NATO Information Management Policy and complements the Policy on Management of Non-Classified NATO Information which addresses the basic principles and standards to be applied within NATO civil and military bodies and NATO member nations for the protection of non-classified NATO information.

1.3. Communication and Information System Security (CIS Security) is one of the elements of Information Assurance (Figure 1) and is defined as the application of security measures for the protection of communication, information and other electronic systems², and the information that is stored, processed or transmitted³ in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.

¹ Med systemstödjande tjänster och resurser avses de tjänster och resurser som krävs för att säkerställa att säkerhetsmålen för kommunikations- och informationssystem (CIS) nås; tjänsterna och resurserna innefattar till exempel kryptoprodukter och krypteringsmekanismer, Comsec-material, katalogtjänster samt arrangemang för och kontroll av användarmiljön.

¹ Supporting System Services and Resources - those services and resources required to ensure that the security objectives of the CIS are achieved; to include, for example, cryptographic products and mechanisms, COMSEC materials, directory services, and environmental facilities and controls.

² Nedan i denna bilaga *kommunikations- och informationssystem*.

² Hereafter referred to within this Enclosure as CIS.

³ Nedan i denna bilaga hantera.

³ Hereafter referred to within this Enclosure as handled.

1.4. För att nå säkerhetsmålen konfidentialitet, riktighet, tillgänglighet, autentisering och oavvislighet⁴ för säkerhetskyddsklassificerad information som hanteras i dessa kommunikations- och informationssystem (CIS) ska en väl avvägd uppsättning säkerhetsåtgärder (fysisk säkerhet, personalsäkerhet, informationssäkerhet och säkerhet i kommunikations- och informationssystem) genomföras för att skapa en säker driftsmiljö för systemen. När säkerhetskyddsklassificerad information med stöd av kontrakt hanteras av industrin, ska ytterligare särskilda industrisäkerhetsåtgärder vidtas i enlighet med bilaga G till denna C-M-handling och det stödjande direktivet om industrisäkerhet.

1.4. In order to achieve the security objectives of confidentiality, integrity, availability, authentication and non-repudiation⁴ for classified information handled in these CIS, a balanced set of security measures (physical, personnel, information and CIS) shall be implemented to create a secure environment in which to operate a CIS. Where classified information is handled by industry in contracts, additional specific industrial security measures shall be applied in accordance with Enclosure G of this C-M and the supporting industrial security directive.

[*Figur i slutet av dokumentet]

[*Figure at the end of the document]

Figur 1 – Förhållandet mellan informationssäkring och säkerhet i kommunikations- och informationssystem (CIS Security)

Figure 1 - Relationship between Information Assurance and CIS Security

1.5. I det primära direktivet om säkerhet i kommunikations- och informationssystem (CIS Security), som offentliggjorts av säkerhetskommittén (SC) och samråds- och ledningsnämnden (C3B) till stöd för denna strategi, behandlas säkerhetsåtgärder i kommunikations- och informationssystem under systemens livscykel samt kommittéernas och Natos civila och militära organs ansvar för säkerheten i systemen. Det primära direktivet om säkerhet i kommunikations- och informationssystem stöds av direktiv som gäller ledning av säkerheten i kommunikations- och informationssystem (inklusive hantering av säkerhetsrisker, säkerhetsackreditering, säkerhetsrelaterad dokumentation och säkerhetsöversyn/säkerhetsinspektion) och aspekter på teknik och genomförande när det gäller säkerheten i kommunikations- och informationssystem (inklusive datorsäkerhet

1.5. The “Primary Directive on CIS Security”, which is published by the SC and the C3B in support of this policy, addresses the CIS Security activities in the CIS life-cycle, and the CIS Security responsibilities of committees, and NATO civil and military bodies. The “Primary Directive on CIS Security” is supported by directives addressing CIS Security management (including security risk management, security accreditation, security-related documentation, and security review / inspection) and CIS Security technical and implementation aspects (including computer and local area network (LAN) security, interconnection of networks security, cryptographic security, transmission security, and emission security).

⁴ Nedan i denna bilaga säkerhetsmål.

⁴ Hereafter referred to within this Enclosure as Security Objectives.

och säkerhet i lokala nätverk (LAN), säkerhet vid sammankoppling av nät, kryptografisk säkerhet, överföringssäkerhet och sändningssäkerhet).

2. SÄKERHETSMÅL

2.1. För att nå tillräcklig säkerhet för Natos säkerhetsskyddsklassificerade information som hanteras i kommunikations- och informationssystem (CIS) ska en väl avvägd uppsättning säkerhetsåtgärder (fysisk säkerhet, personalsäkerhet, informationssäkerhet och säkerhet i kommunikations- och informationssystem) identifieras och genomföras för att skapa en säker miljö för driften av kommunikations- och informationssystem och för att nå följande säkerhetsmål:

- a) säkerställa konfidentialiteten för Natos säkerhetsskyddsklassificerade information genom att kontrollera röjandet av och åtkomsten till information samt för systemstödjande tjänster och resurser,
- b) säkerställa riktigheten hos Natos säkerhetsskyddsklassificerade information och systemstödjande tjänster och resurser,
- c) säkerställa tillgängligheten till Natos säkerhetsskyddsklassificerade information och systemstödjande tjänster och resurser,
- d) säkerställa tillförlitlig identifiering och autentisering av personer, utrustning och tjänster som har åtkomst till kommunikations- och informationssystem där Natos säkerhetsskyddsklassificerade information hanteras, och
- e) säkerställa lämplig oavvislighet för personer och enheter som har behandlat informationen.

2.2. Natos säkerhetsskyddsklassificerade information samt systemstödjande tjänster och resurser ska skyddas genom en minimiuppsättning åtgärder som syftar till att säkerställa allmänt skydd mot vanligt förekommande problem (oavsiktliga eller avsiktliga) som är kända för att påverka alla system samt systemstödjande tjänster och resurser. Ytterligare åtgärder ska vidtas, med hänsyn till omständigheterna, om det vid en säkerhetsriskbedömning har fastställts att Natos

2. SECURITY OBJECTIVES

2.1. To achieve adequate security protection of NATO classified information handled in CIS, a balanced set of security measures (physical, personnel, information and CIS) shall be identified and implemented to create a secure environment in which a CIS operates, and to meet the following security objectives:

- (a) to ensure the confidentiality of information by controlling the disclosure of, and access to, NATO classified information, and supporting system services and resources;
- (b) to ensure the integrity of NATO classified information, and supporting system services and resources;
- (c) to ensure the availability of NATO classified information, and supporting system services and resources;
- (d) to ensure the reliable identification and authentication of persons, devices and services accessing CIS handling NATO classified information; and
- (e) to ensure appropriate non-repudiation for individuals and entities having processed the information.

2.2. NATO classified information and supporting system services and resources, shall be protected by a minimum set of measures aimed at ensuring general protection against commonly encountered problems (whether accidental or intentional) known to affect all systems and supporting system services and resources. Additional measures shall be taken, appropriate to the circumstances, where a security risk assessment has established that NATO classified information

säkerhetsskyddsklassificerade information och/eller systemstödande tjänster och resurser utsätts för ökade risker till följd av särskilda hot och sårbarheter.

2.3. Oberoende av säkerhetsskyddsklassificeringen av den Natoinformation som hanteras ska Natos säkerhetsmyndigheter bedöma de risker och den skadenivå som åsamkas Nato om åtgärderna för att nå säkerhetsmålen för icke-konfidentialitet inte fungerar. Minimiuppsättningen åtgärder för icke-konfidentiella tjänster ska fastställas i enlighet med direktiv som stöder denna strategi.

3. SÄKERHETSACKREDITERING

3.1. I vilken utsträckning säkerhetsmålen ska nås och i vilken utsträckning säkerhetsåtgärder behövs i kommunikations- och informationssystem (CIS) för att skydda säkerhetsskyddsklassificerad Natoinformation och systemstödande tjänster och resurser ska fastställas vid förfarandet för fastställande av säkerhetskravet. Genom förfarandet för säkerhetsackreditering fastställs det att en tillräcklig skyddsnivå har nåtts och upprätthålls.

3.2 Alla kommunikations- och informationssystem (CIS) där Natos säkerhetsskyddsklassificerade information hanteras ska omfattas av ett förfarande för säkerhetsackreditering som fokuserar på säkerhetsmålen

4. PERSONALSÄKERHET

4.1. Personer som är behöriga att ha åtkomst till Natos säkerhetsskyddsklassificerade information i någon form ska i förekommande fall säkerhetsprövas med beaktande av deras övergripande ansvar för att nå säkerhetsmålen för informationen och de systemstödande tjänsterna och resurserna. Detta innefattar personer som är behöriga att ha åtkomst till systemstödande tjänster och resurser eller som ansvarar för skyddet av systemen, även om personerna inte är behöriga att ha åtkomst till den information som hanteras i systemen.

and/or supporting system services and resources are subject to increased risks from specific threats and vulnerabilities.

2.3. Independent of the security classification of the NATO information being handled, NATO security authorities shall assess the risks and the level of damage done to NATO if the measures to achieve the non-confidentiality security objectives fail. The minimum set of measures for nonconfidentiality services shall be determined in accordance with directives supporting this policy.

3. SECURITY ACCREDITATION

3.1. The extent to which the security objectives are to be met, and the extent to which CIS Security measures are to be relied upon for the protection of NATO classified information and supporting system services and resources shall be determined during the process of establishing the security requirement. The security accreditation process shall determine that an adequate level of protection has been achieved, and is being maintained.

3.2 All CIS handling NATO classified information shall be subject to a security accreditation process, addressing the Security Objectives.

4. PERSONNEL SECURITY

4.1. Individuals authorised access to NATO classified information in any form shall be security cleared, where appropriate, taking account of their aggregate responsibility for achieving the Security Objectives of the information and the supporting system services and resources. This includes individuals who are authorised access to supporting system services and resources, or who are responsible for their protection, even if they are not authorised access to the information handled by the system.

5. FYSISK SÄKERHET

5.1. Utrymmen där Natos säkerhetsskyddsklassificerade information presenteras eller hanteras med hjälp av informationsteknik eller där det är möjligt att få åtkomst till sådan information ska inrättas så att det övergripande kravet för säkerhetsmålen uppfylls.

6. INFORMATIONSSÄKERHET

6.1. Alla säkerhetsskyddsklassificerade lagringsmedier för datorer ska vara korrekt identifierade, lagrade och skyddade på ett sätt som motsvarar den högsta säkerhetsskyddsklassificeringsnivån för den lagrade informationen.

6.2. Natos säkerhetsskyddsklassificerade information som lagrats på återanvändbara lagringsmedier för datorer får raderas endast i enlighet med förfaranden som godkänts av den behöriga säkerhetsmyndigheten.

6.3. Godkända säkerhetsåtgärder (konfidentialitet och icke-konfidentialitet) som genomförs i enlighet med direktiv som stöder denna strategi får användas för att skydda Natos säkerhetsskyddsklassificerade information i lagringsmedier för datorer på ett sätt som sänker de fysiska säkerhetskraven så att de motsvarar en lägre säkerhetsskyddsklassificeringsnivå.

7. INDUSTRISSÄKERHET

7.1. Det ska fastställas att en entreprenörs verksamhetsställe som används för genomförande av kontrakt och där Natos säkerhetsskyddsklassificerade information (CIS) hanteras i kommunikations- och informationssystem uppfyller det övergripande kravet för säkerhetsmålen.

7.2. En konsekvent uppsättning säkerhetsåtgärder för kommunikations- och informationssystem (CIS) ska beskrivas i kontrakt, tilläggs klausuler om säkerhet (SAL) och/eller säkerhetsinsanvisningar för projekt (PSI) och/eller servicenivåavtal (SLA), beroende på vad som är tillämpligt, och genomförs av entreprenörerna för att nå säkerhetsmålen

5. PHYSICAL SECURITY

5.1. Areas in which NATO classified information is presented or handled using information technology, or where potential access to such information is possible, shall be established such that the aggregate requirement for the Security Objectives is met.

6. SECURITY OF INFORMATION

6.1. All classified computer storage media shall be properly identified, stored and protected in a manner commensurate with the highest classification of the stored information.

6.2. NATO classified information recorded on re-usable computer storage media, shall only be erased in accordance with procedures approved by the appropriate security authority.

6.3. Approved security measures (confidentiality and non-confidentiality), implemented in accordance with directives supporting this policy, may be used to protect NATO classified information in computer storage media in such a manner as to reduce the physical security requirements commensurate with a lower classification level.

7. INDUSTRIAL SECURITY

7.1. A contractor facility used for contracts in which NATO classified information is handled on CIS shall be established to meet the aggregate requirement for the Security Objectives.

7.2. A consistent set of CIS security measures shall be described in contracts, Security Aspect Letters (SAL) and/or Project Security Instructions (PSI) and/or Service Level Agreements (SLA), as applicable, and be implemented by contractors to meet the NATO CIS security objectives and to protect NATO classified information and supporting services.

för Natos kommunikations- och informationssystem och för att skydda Natos säkerhetsskyddsklassificerade information och stödjande tjänster.

8. SÄKERHETSÅTGÄRDER

8.1. För alla kommunikations- och informationssystem (CIS) där Natos säkerhetsskyddsklassificerade information hanteras ska en konsekvent uppsättning säkerhetsåtgärder tillämpas för att nå säkerhetsmålen och skydda information samt systemstödjande tjänster och resurser. Säkerhetsåtgärderna ska, i tillämpliga delar, omfatta följande:

- a) sådana sätt att tillhandahålla tillräcklig information för att kunna undersöka ett avsiktligt, oavsiktligt eller försök till äventyrande av säkerhetsmålen för säkerhetsskyddsklassificerad information och systemstödjande tjänster och resurser som står i proportion till den skada som skulle uppstå,
- b) sätt att på ett tillförlitligt sätt identifiera och autentisera personer, utrustning och tjänster som är behöriga att ha åtkomst. Information och material som kontrollerar tillträdet till ett kommunikations- och informationssystem ska kontrolleras och skyddas med arrangemang som står i proportion till den information som tillträdet kan ge åtkomst till. I Natos kommunikations- och informationssystem ska starka autentiseringsmekanismer för personer tillämpas,
- c) sätt att utifrån principen om behovslenig behörighet kontrollera röjandet av och åtkomsten till Natos säkerhetsskyddsklassificerade information samt systemstödjande tjänster och resurser,
- d) sätt att säkerställa riktigheten av och ursprunget för Natos säkerhetsskyddsklassificerade information samt systemstödjande tjänster och resurser,
- e) sätt att upprätthålla riktigheten av Natos säkerhetsskyddsklassificerade information samt systemstödjande tjänster och resurser,

8. SECURITY MEASURES

8.1. For all CIS handling NATO classified information, a consistent set of security measures shall be applied to meet the Security Objectives to protect information and supporting system services and resources. The security measures shall include, where appropriate, the following:

- (a) a means to provide sufficient information to be able to investigate a deliberate, accidental or attempted compromise of the security objectives of classified information and supporting system services and resources, commensurate with the damage that would be caused;
- (b) a means to reliably identify and authenticate persons, devices and services authorised access. Information and material which controls access to a CIS shall be controlled and protected under arrangements commensurate with the information to which it may give access. On NATO CIS strong authentication mechanisms for persons shall be implemented;
- (c) a means to control disclosure of, and access to, NATO classified information and supporting system services and resources, based upon the need-to-know principle;
- (d) a means to verify the integrity and origin of NATO classified information, and supporting system services and resources;
- (e) a means to maintain the integrity of NATO classified information and supporting system services and resources;

f) sätt att upprätthålla åtkomsten till Natos säkerhetsskyddsklassificerade information samt systemstödande tjänster och resurser,

g) sätt att kontrollera förbindelsen för kommunikations- och informationssystem där Natos säkerhetsskyddsklassificerade information hanteras,

h) fastställande av förtroendet för skyddsmekanismerna för säkerhet i kommunikations- och informationssystem (CIS Security),

i) sätt att utvärdera och kontrollera att skyddsmekanismerna för säkerhet i kommunikations- och informationssystem fungerar under systemets livscykel,

j) sätt att undersöka användaraktiviteten och aktiviteten i kommunikations- och informationssystem,

k) sätt att tillhandahålla garantier för oavvislighet så att avsändaren av informationen får bevis på leverans och att mottagaren får bevis på avsändarens identitet, och

l) sätt att skydda Natos säkerhetsskyddsklassificerade och lagrade information om de fysiska säkerhetsåtgärderna inte uppfyller miniminormerna.

8.2. Mekanismer och förfaranden för säkerhetshantering ska finnas för att avskräcka, förhindra, upptäcka, motstå och avhjälpa följderna av incidenter som påverkar säkerhetsmålen för Natos säkerhetsskyddsklassificerade information och systemstödande tjänster och resurser, inbegripet rapportering av säkerhetsincidenter.

8.3. Säkerhetsåtgärderna ska ledas och genomföras i enlighet med direktiv som stöder denna strategi.

9. RISKHANTERING

9.1. Kommunikations- och informationssystem (CIS) där Natos säkerhetsskyddsklassificerade information hanteras inom Natos civila och militära organ ska omfattas av sä-

(f) a means to maintain the availability of NATO classified information and supporting system services and resources;

(g) a means to control the connection of CIS handling NATO classified information;

(h) a determination of the confidence to be placed in the protection mechanisms of CIS Security;

(i) a means to assess and verify the proper functioning of the protection mechanisms of CIS Security over the life-cycle of the CIS;

(j) a means to investigate user and CIS activity;

(k) a means to provide non-repudiation assurances that the sender of information is provided with proof of delivery and the recipient is provided proof of the sender's identity; and

(l) a means to protect stored NATO classified information where the physical security measures do not meet the minimum standards.

8.2. Security management mechanisms and procedures shall be in place to deter, prevent, detect, withstand, and recover from, the impacts of incidents affecting the Security Objectives of NATO classified information and supporting system services and resources, including the reporting of security incidents.

8.3. The security measures shall be managed and implemented in accordance with directives supporting this policy.

9. SECURITY RISK MANAGEMENT

9.1. CIS handling NATO classified information, in NATO civil and military bodies, shall be subject to security risk management, including security risk assessment, in accordance with the requirements

kerhetsriskhantering, inbegripet säkerhetsriskbedömning, i enlighet med kraven i direktiv som stöder denna strategi.

9.2. Säkerhetsriskhantering av Natos kommunikations- och informationssystem (CIS) ska säkerställa kontinuerlig bedömning av systemens sårbarheter och säkerhetsöverensstämmelse och ska övergå till dynamisk riskhantering för att effektivt kunna reagera på de utmaningar som dagens komplexa driftscenarier och mångfasetterade hotmiljöer medför.

10. ELEKTROMAGNETISK ÖVERFÖRING⁵ AV NATOS SÄKERHETSSKYDDSKLASSIFICERADE INFORMATION

10.1. När Natos säkerhetsskyddsklassificerade information överförs elektromagnetiskt ska särskilda åtgärder genomföras så att säkerhetsmålen för sådana överföringar nås. Natos myndigheter ska fastställa kraven för att skydda överföringar från upptäckt, avlyssning eller utnyttjande.

11. KRYPTOGRAFISK SÄKERHET

11.1. När kryptografiska produkter eller mekanismer krävs för att tillhandahålla konfidentiellt och icke-konfidentiellt skydd, oavsett om det gäller överföring, behandling eller lagring av information (data i vila), ska produkterna eller mekanismerna vara särskilt godkända för ändamålet och särskilda kryptografiska krav för fysiska, förfarandemässiga och tekniska åtgärder ska genomföras för att nå de säkerhetsmål som krävs.

11.2. Data i vila ska skyddas på den nivå som krävs i enlighet med säkerhetsmålen och om kryptografiska produkter eller mekanismer används ska kraven på kryptografisk säkerhet vara i enlighet med Natos relevanta direktiv om teknik och genomförande.

of directives supporting this policy.

9.2. Security risk management of NATO CIS shall ensure continuous assessment of system vulnerabilities and security compliance and shall move towards dynamic risk management to be able to face effectively the challenges posed by today's complex operational scenarios and multifaceted threat environments.

10. ELECTROMAGNETIC TRANSMISSION⁵ of NATO CLASSIFIED INFORMATION

10.1. When NATO classified information is transmitted electromagnetically, special measures shall be implemented to achieve the Security Objectives of such transmissions. NATO authorities shall determine the requirements for protecting transmissions from detection, interception or exploitation.

11. CRYPTOGRAPHIC SECURITY

11.1. When cryptographic products or mechanisms are required to provide confidentiality and non-confidentiality protection, whether during information transmission, processing or storage (data at rest), such products or mechanisms shall be specifically approved for the purpose and specific cryptographic requirements for physical, procedural and technical measures shall be implemented to achieve the required Security Objectives.

11.2. Data at rest shall be protected to a level adequate to the required Security Objectives, and, where cryptographic products and mechanisms are used, the requirements

⁵ Termen elektromagnetisk överföring omfattar överföring av både elektrisk och magnetisk karaktär eller med sådana egenskaper och omfattar bland annat synligt ljus, radiovågor, mikrovågor och infraröd strålning.

⁵ The term "electromagnetic transmission" covers transmission having both an electrical and magnetic character or properties, and includes, inter alia, visible light, radio waves, microwave, and infrared radiation

- for cryptographic security shall be in accordance with the relevant NATO Technical and Implementation Directives.
- 11.3. Under överföringen ska konfidentialiteten för information som säkerhetskyddsklassificerats som NATO SECRET eller högre skyddas med kryptografiska produkter eller mekanismer som godkänts av Natos militärkommitté (NAMILCOM).
- 11.3. During transmission, the confidentiality of information classified NS and above shall be protected by cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM).
- 11.4. Under överföringen ska konfidentialiteten för information som säkerhetskyddsklassificerats som NATO CONFIDENTIAL eller NATO RESTRICTED skyddas med kryptografiska produkter eller mekanismer som godkänts av antingen Natos militärkommitté (NAMILCOM) eller en medlemsstat i Nato.
- 11.4. During transmission, the confidentiality of information classified NC or NR shall be protected by cryptographic products or mechanisms approved by either the NAMILCOM or a NATO member nation.
- 11.5. Under överföringen ska kraven på icke-konfidentialitet säkerställas i enlighet med driftskraven för kommunikationssystemet. Utvärderingskraven och godkännandemyndigheten för icke-konfidentiella mekanismer baserade på kryptografi ska identifieras och överenskommas i samband med specifikationen av sådana mekanismer i driftskravet, i enlighet med vad som överenskomits i tekniska direktiv.
- 11.5. During transmission, the non-confidentiality requirements shall be assured in accordance with the communications system's operational requirement. The evaluation requirements and approval authority, for non-confidentiality mechanisms based on cryptography, shall be identified and agreed in conjunction with the specification of such mechanisms in the operational requirement, as agreed in technical directives.
- 11.6. Under exceptionella operativa omständigheter får information som säkerhetskyddsklassificerats som NATO CONFIDENTIAL eller NATO SECRET överföras i klartext under förutsättning att varje tillfälle vederbörligen rapporteras till de högre myndigheterna. De exceptionella omständigheterna är följande:
- 11.6. Under exceptional operational circumstances, information classified NC and NS may be transmitted in clear text provided each occasion is properly reported to the higher authorities. The exceptional circumstances are as follows:
- a) under en överhängande eller faktisk kris eller konflikt eller i krigssituationer, och
 - a) during impending or actual crisis, conflict, or war situations; and
 - b) när leveranshastigheten är av största vikt, inga krypteringsmetoder finns att tillgå och det bedöms att den överförda informationen inte kan utnyttjas i tid för att påverka verksamheten negativt.
 - (b) when speed of delivery is of paramount importance, means of encryption are not available and it is assessed that the transmitted information cannot be exploited in time to adversely influence operations.

11.7. Under exceptionella operativa omständigheter när leveranshastigheten är av största vikt, inga krypteringsmetoder finns att tillgå och det bedöms att den överförda informationen inte kan utnyttjas i tid för att påverka verksamheten negativt, får information som säkerhetsskyddsklassificerats som NATO RESTRICTED överföras i klartext.

11.8. Under överföring mellan Nato och kommunikations- och informationssystem (CIS) hos stater eller internationella organisationer som inte hör till Nato (NNN/IO) ska konfidentialiteten för information som säkerhetsskyddsklassificerats som NATO SECRET eller högre skyddas med kryptografiska produkter eller mekanismer som godkänts av Natos militärkommitté (NAMILCOM).

11.9. Under överföring inom kommunikations- och informationssystem (CIS) i stater eller internationella organisationer som inte hör till Nato (NNN/IO) ska konfidentialiteten för information som säkerhetsskyddsklassificerats som NATO SECRET eller högre skyddas med kryptografiska produkter eller mekanismer som godkänts av Natos militärkommitté (NAMILCOM).

11.10. Om kraven i punkterna 11.8 och 11.9 inte kan uppfyllas kan Nato och en internationell organisation (IO) komma överens om ömsesidigt godkännande av varandras bedömnings-, urvals- och godkännandeprocesser för kryptografiska produkter eller mekanismer som är godkända för skydd vid överföring av information som säkerhetsskyddsklassificerats som NATO SECRET eller den internationella organisationens information på motsvarande säkerhetsskyddsklassificeringsnivå. Villkoren för ett sådant godkännande anges i punkt 11.12.

11.11. Vid exceptionella omständigheter och för att stödja särskilda driftskrav och om kraven enligt punkterna 11.8 och 11.9 inte kan uppfyllas, får Nato samtycka till bedömnings-, urvals- och godkännandeprocesserna för en stat utanför Nato (NNN) när det gäller kryptografiska produkter eller mekanismer

11.7. Under exceptional operational circumstances, when speed is of paramount importance, means of encryption are not available and it is assessed that the transmitted information cannot be exploited in time to adversely influence operations, information classified NR may be transmitted in clear text.

11.8. During transmission between NATO and non-NATO nations / International Organisations (NNN/IO) CIS, the confidentiality of information classified NS and above shall be protected by cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM).

11.9. During transmission within NNN/IO CIS, the confidentiality of information classified NS and above shall be protected by cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM).

11.10. Where the requirements of paragraphs 11.8 and 11.9 above cannot be met, NATO and an IO may reach agreement on the mutual acceptance of each others' evaluation, selection and approval processes for cryptographic products or mechanisms authorised for the protection in transmission of NS information or IO information of the equivalent classification level. The conditions for such acceptance are set out in paragraph 11.12 below.

11.11. In exceptional circumstances, in order to support specific operational requirements, and where the requirements of paragraphs 11.8 and 11.9 above cannot be met, NATO may agree the NNN's evaluation, selection and approval processes for cryptographic products or mechanisms authorised

som är godkända för att skydda överföringen av information som säkerhetsskyddsklassificerats som NATO SECRET eller information på motsvarande säkerhetsskyddsklassificeringsnivå från staten utanför Nato. Villkoren för ett sådant samtycke anges i punkt 11.12.

11.12. Följande villkor är tillämpliga på de situationer som beskrivs i punkterna 11.10 och 11.11:

a) en stat eller internationell organisation som inte hör till Nato (NNN/IO) ska ha ett säkerhetsavtal med Nato och ett intyg utfärdat av Natos säkerhetsbyrå (NOS) på att den på lämpligt sätt kan skydda Natos utlämnade säkerhetsskyddsklassificerade information,

b) varje stat eller internationell organisation som inte hör till Nato ska behandlas från fall till fall och grunden för varje godkännande/avtal ska anges i de säkerhetsarrangemang som stöder säkerhetsavtalet mellan Nato och den stat eller den internationella organisation som inte hör till Nato,

c) villkoren för ett sådant godkännande/avtal ska godkännas av Natos militärkommitté (NAMILCOM) på grundval av en objektiv bedömning av Natos säkerhetsbyrå i samarbete med Natos militärkommittés byrå för bedömning av säkerhet i och utvärdering av kommunikations- och informationssystem (SECAN), samråds- och ledningsnämndens (C3B) panel för informationssäkring och cyberförsvarskapacitet samt samråds- och ledningspersonalen vid Natos högkvarter (NATO HQ C3) när det gäller förmågan hos den stat eller den internationella organisation som inte hör till Nato att utföra kryptografiska bedömningar som uppfyller krav som är likvärdiga med dem som används inom Nato för det kryptografiska skyddet av information som säkerhetsskyddsklassificerats som NATO SECRET, och

d) Natos säkerhetsbyrå ska i samarbete med byrån för bedömning av säkerhet i

for the protection in transmission of NS information or NNN information of the equivalent classification level. The conditions for such agreement are set out in paragraph 11.12 below.

11.12. The following conditions are applicable in respect to the scenarios described at paragraphs 11.10 and 11.11 above:

(a) the NNN/IO shall have a Security Agreement with NATO and be certified by the NATO Office of Security (NOS) that they can appropriately protect released NATO classified information;

(b) each NNN/IO shall be treated on a case-by-case basis; and the basis of any acceptance / agreement shall be set out in the security arrangements supporting the Security Agreement between NATO and the NNN/IO;

(c) the terms of any such acceptance / agreement shall be approved by the NAMILCOM on the basis of an objective assessment carried out by the NOS, working in conjunction with the NAMILCOM Communications and Information Systems Security and Evaluation Agency (SECAN), the C3B Information Assurance and Cyber Defence Capability Panel and the NATO HQ C3 Staff, of the capability of the NNN/IO to perform cryptographic evaluations that meet requirements equivalent to those used within NATO for the cryptographic protection of NS information; and

(d) the NOS, in conjunction with SECAN and the NATO HQ C3 Staff, shall satisfy

och utvärdering av kommunikations- och informationssystem och samråds- och ledningspersonalen vid Natos högkvarter genom kontroller och periodiskt återkommande kontroller förvissa sig om att den stat eller den internationella organisation som inte hör till Nato har inrättat lämpliga strukturer, regler och förfaranden för bedömningen, urvalet, godkännandet och kontrollen av kryptografiska produkter och mekanismer och att dessa strukturer, regler och förfaranden tillämpas effektivt och säkert i praktiken.

11.13. Vid godkännande eller överenskommelse i enlighet med villkoren i punkt 11.12 får konfidentialiteten för information som säkerhetsskyddsklassificerats som NATO SECRET skyddas med antingen kryptografiska produkter eller mekanismer som godkänts av Natos militärkommitté (NAMILCOM) eller kryptografiska produkter eller mekanismer som godkänts för skyddet på motsvarande säkerhetsskyddsklassificeringsnivå av den nationella säkerhetsmyndigheten för kommunikations- och informationssystem (NCSA) eller en motsvarande myndighet i den stat eller den internationella organisation som inte hör till Nato (NNN/IO).

11.14. Under överföring mellan Nato och kommunikations- och informationssystem (CIS) hos stater eller internationella organisationer som inte hör till Nato (NNN/IO) samt inom kommunikations- och informationssystem hos stater eller internationella organisationer som inte hör till Nato ska konfidentialiteten för information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller NATO RESTRICTED skyddas med kryptografiska produkter eller mekanismer som godkänts av en behörig myndighet. Den behöriga myndigheten kan vara Natos militärkommitté (NAMILCOM), den nationella säkerhetsmyndigheten för kommunikations- och informationssystem (NCSA) i en medlemsstat i Nato eller den motsvarande myndigheten i en stat eller internationell organisation som inte hör till Nato, förutsatt att staten eller den internationella organisationen har

themselves, through verification and periodic re-verification, that the NNN/IO has in place appropriate structures, rules and procedures for the evaluation, selection, approval and control of cryptographic products and mechanisms, and that those structures, rules and procedures are being effectively and securely applied in practice.

11.13. Where acceptance / agreement is reached in accordance with the conditions set out in paragraph 11.12 above, the confidentiality of information classified NS may be protected by either cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM) or cryptographic products or mechanisms approved by the NCSA (or equivalent authority) of the NNN/IO for the protection of the equivalent classification level.

11.14. During transmission between NATO and NNN/IO CIS and within NNN/IO CIS, the confidentiality of information classified NC or NR shall be protected by cryptographic products or mechanisms evaluated and approved by an appropriate authority. The appropriate authority may be the NAMILCOM, the NCSA of a NATO member nation or the equivalent authority of the NNN/IO, provided that the NNN/IO has appropriate structures, rules and procedures in place for the evaluation, selection, approval and control of such products or mechanisms, and that those structures, rules and procedures are being effectively and securely applied in practice. The structures, rules and procedures shall be agreed between the NAMILCOM and the NNN/IO.

inrättat lämpliga strukturer, regler och förfaranden för bedömningen, urvalet, godkännandet och kontrollen av sådana produkter eller mekanismer och att dessa strukturer, regler och förfaranden tillämpas effektivt och säkert i praktiken. Natos militärkommitté och den stat eller den internationella organisation som inte hör till Nato ska komma överens om strukturerna, reglerna och förfarandena.

11.15. Den känsliga karaktären hos det kryptomaterial som används för att skydda Natos säkerhetsskyddsklassificerade information gör det nödvändigt att vidta särskilda försiktighetsåtgärder i fråga om säkerhet utöver de som krävs för att skydda annat slag av Natos säkerhetsskyddsklassificerade information.

11.16. Det skydd som ska ges kryptomaterial ska motsvara den skada som kan orsakas om skyddet skulle sluta fungera. Det ska finnas positiva metoder för att bedöma och kontrollera skyddet för kryptografiska produkter och mekanismer och att de fungerar samt skyddet för och kontrollen av kryptografisk information (till exempel tillämpningsdetaljer med tillhörande dokumentation).

11.17. Med hänsyn till den särskilda känsligheten hos kryptografisk information ska särskilda bestämmelser och organ finnas inom Nato och varje medlemsstat för att reglera mottagandet, kontrollen och spridningen av Natos kryptografiska information till särskilt certifierade personer.

11.18. Särskilda förfaranden som reglerar delning av teknisk information och som reglerar urval, produktion och upphandling av kryptografiska produkter och mekanismer ska också följas.

12. SÄNDNINGSSÄKERHET

12.1. Säkerhetsåtgärder ska genomföras för att skydda information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller högre mot läckor genom

11.15. The sensitive nature of the cryptomaterial used to protect NATO classified information necessitates the application of special security precautions beyond those required for the protection of other NATO classified information.

11.16. The protection which shall be afforded to cryptomaterial shall be commensurate with the damage that may be caused should that protection fail. There shall be positive means to assess and verify the protection and proper functioning of the cryptographic products and mechanisms, and the protection and control of cryptographic information (e.g. implementation details and associated documentation).

11.17. In recognition of the particular sensitivity of cryptographic information, special regulations and bodies shall exist within NATO and within each member nation to govern the receipt, control and dissemination of NATO cryptographic information to specially certified persons.

11.18. Special procedures shall also be followed which regulate the sharing of technical information, and which regulate the selection, production and procurement of cryptographic products and mechanisms.

12. EMISSION SECURITY

12.1. Security measures shall be implemented to protect against the compromise of information classified NC and above through unintentional electromagnetic emissions. The measures shall be commensurate

oavsiktlig elektromagnetisk strålning. Åtgärderna ska motsvara spridningsrisken och informationens känslighet.

with the risk of exploitation and the sensitivity of the information.

13. SÄRSKILT SÄKERHETSANSVAR FÖR KOMMUNIKATIONS- OCH INFORMATIONSSYSTEM

13. SPECIFIC CIS SECURITY RESPONSIBILITIES

13.1 Natos militärkommitté (NAMILCOM)

13.1 NATO Military Committee (NAMILCOM)

13.1.1. Natos militärkommittés ansvar för säkerheten i kommunikations- och informationssystem (CIS Security) innefattar säkerhetsgodkännande och frisläppande av kryptografisk utrustning samt deltagande i bedömningen och urvalet av kryptografiska produkter och mekanismer för Natos standardiserade användning. Militärkommitténs fyra nationellt bemannade byråer (byrån för bedömning av säkerhet i och utvärdering av kommunikations- och informationssystem (SECAN), byrån för distribution och revision (DACAN), europeiska byrån för kommunikationssäkerhet och utvärdering (EUSEC) och europeiska byrån för distribution och revision (EUDAC)) ger i fråga om säkerheten i kommunikations- och informationssystem (CIS Security) råd och stöd till Natos militärkommitté, säkerhetskommittén (SC) och samråds- och ledningsnämnden (C3B) samt, i förekommande fall, till deras understrukturer, till medlemsstater och till andra Natoorganisationer.

13.1.1. The NAMILCOM's responsibilities on CIS Security include the security approval and release of cryptographic equipment and participating in the evaluation and selection of cryptographic products and mechanisms for standard NATO use. The four nationally manned agencies of the Military Committee (SECAN, DACAN, EUSEC and EUDAC) provide advice and support on CIS Security to the NAMILCOM, to the SC, to the C3B and, as appropriate, to their substructures, to member nations and to other NATO organisations.

13.2. Samråds- och ledningsnämnden (C3B)

13.2. C3 Board (C3B)

13.2.1. I egenskap av alliansens högsta strategikommitté för samråd och ledning (C3) stöder samråds- och ledningsnämnden (C3B) Natos militärkommitté (NAMILCOM) och Natos politiska myndigheter i deras valideringsprocess när det gäller förmågor och projekt inom samråd och ledning genom översyn av driftskraven för samråd och ledning. Samråds- och ledningsnämnden ansvarar för tillhandahållandet av säkra och interoperabla Natoomfattande system för samråd och ledning. Personalstöd till samråds- och ledningsnämnden ges av personalen för konsultation och ledning vid Natos högkvarter (NHQC3S).

13.2.1. As the senior Consultation, Command and Control (C3) policy committee within the Alliance, the C3B supports the NAMILCOM and the NATO political authorities in their validation process for C3 capabilities and projects by reviewing operational C3 requirements. The C3B is responsible for the provision of secure and interoperable NATO-wide C3 systems. Staff support to the C3B is provided by the NATO HQ C3 Staff (NHQC3S).

13.3. Natos styrgrupp för cyberförsvar (CDMB)

13.3.1 Styrgruppen för cyberförsvar är det samordningsorgan för cyberförsvar som svarar för strategisk planering och styrning av genomförandet av strategin för cyberförsvar och främjar samarbetet med de allierade. Styrgruppen för cyberförsvar rapporterar till och får politisk styrning från Nordatlantiska rådet (NAC) genom kommittén för försvars- politik och försvarsplanering i förstärkt form (DPPC (R)). Styrgruppen för cyberförsvar övervakas av de allierade genom samråds- och ledningsnämnden (C3B) när det gäller strategin för samråd och ledning (C3) samt aspekter på genomförandet av cyberförsvar. Styrgruppen för cyberförsvar samråder i särskilda frågor via lämpliga Natokommittéer.

13.4. Nationell säkerhetsmyndighet för kommunikations- och informationssystem (NCSA)

13.4.1. Varje medlemsstat i Nato, och i tillämpliga fall stater utanför Nato, ska fastställa en nationell säkerhetsmyndighet för kommunikations- och informationssystem (NCSA) som får inrättas som en byrå inom den nationella säkerhetsinfrastrukturen. Den nationella säkerhetsmyndigheten för kommunikations- och informationssystem svarar för att

- a) kontrollera kryptografisk teknisk information i anslutning till skyddet av Natoinformation i staten i fråga,
- b) se till att kryptografiska system, produkter och mekanismer som används för att skydda Natoinformation väljs, används och underhålls som sig bör,
- c) se till att säkerhetsprodukter som används för att skydda Natoinformation i kommunikations- och informationssystem (CIS) väljs, används och underhålls som sig bör i den egna staten,
- d) informera behöriga Natoorgan och nationella organ, både civila och militära, om kommunikationssäkerhet och tekniska frå-

13.3. NATO Cyber Defence Management Board (CDMB)

13.3.1 The CDMB is the cyber defence co-ordination body providing strategic planning and direction for the implementation of the Cyber Defence Policy and facilitating cooperation with Allies. The CDMB reports to and receive political guidance from the NAC through the Defence Policy and Planning Committee in reinforced format (DPPC(R)). The CDMB is supervised by Allies through the C3B on C3 policy and implementation aspects of cyber defence. CDMB consults on specific subject matters through the appropriate NATO committees.

13.4. National CIS Security Authority (NCSA)

13.4.1. Each NATO and non-NATO nation, where applicable to the latter, shall identify an NCSA, which may be established as an agency in the national security infrastructure. The NCSA is responsible for:

- (a) controlling cryptographic technical information related to the protection of NATO information within their nation;
- (b) ensuring that cryptographic systems, products and mechanisms for protecting NATO information are appropriately selected, operated and maintained;
- (c) ensuring that CIS security products for protecting NATO information are appropriately selected, operated and maintained within their nation;
- (d) communicating on NATO communications security and technical matters on CIS Security, both civil and military,

gor som gäller säkerhet i kommunikations- och informationssystem (CIS Security), och

e) utse en nationell Tempest-myndighet i förekommande fall.

13.4.2. Nationella säkerhetsmyndigheter för kommunikations- och informationssystem (NCSAs) samarbetar med sina nationella säkerhetsmyndigheter (NSA(s)).

13.5. Nationell distributionsmyndighet (NDA)

13.5.1 Varje medlemsstat i Nato, och i tillämpliga fall stater utanför Nato, ska fastställa en nationell distributionsmyndighet som får inrättas som en byrå inom den nationella säkerhetsinfrastrukturen och som ska ansvara för förvaltningen av Natos kryptomaterial i den egna staten och se till att lämpliga förfaranden följs och att kanaler inrättas för heltäckande redovisning, säker hantering, förvaring, distribution och utplåning av allt kryptomaterial.

13.5.2. Nationella distributionsmyndigheter samarbetar med sina nationella säkerhetsmyndigheter (NSA(s)).

13.6. Myndighet(er) för säkerhetsackreditering

13.6.1. Varje medlemsstat i Nato, och i tillämpliga fall en stat utanför Nato, ska fastställa en eller flera myndigheter för säkerhetsackreditering med ansvar för säkerhetsackreditering av följande:

a) nationella kommunikations- och informationssystem (CIS) där Natos säkerhetsskyddsklassificerade information hanteras, och

b) Natos kommunikations- och informationssystem som är i drift inom nationella organ eller organisationer, beroende på vad som är lämpligt för stater utanför Nato.

13.6.2. Om ett civilt eller militärt Natoorgan inrättas i en medlemsstat i Nato ska Natos kommunikations- och informationssystem

with appropriate NATO and national bodies; and

(e) identifying a National TEMPEST Authority, as appropriate.

13.4.2. NCSAs work in co-ordination with their NSA(s).

13.5. National Distribution Authority (NDA)

13.5.1 Each NATO and non-NATO nation, where applicable to the latter, shall identify an NDA, which may be established as an agency in the national security infrastructure, which is responsible for the management of NATO cryptomaterial within their nation and shall ensure that appropriate procedures are enforced and channels established for the comprehensive accounting, secure handling, storage, distribution and destruction of all cryptomaterial.

13.5.2. NDAs work in co-ordination with their NSA(s).

13.6. Security Accreditation Authority(s)

13.6.1. Each NATO and non-NATO nation, where applicable to the latter, shall identify a security accreditation authority(s) which is responsible for the security accreditation of the following:

(a) national CIS handling NATO classified information; and

(b) NATO CIS operating within national bodies / organisations, as appropriate for non-NATO Nations.

13.6.2. Where a NATO civil or military body is established within a NATO nation, the NATO CIS shall be subject to security accreditation by a NATO SAA. In this case,

(CIS) säkerhetsackrediteras av en Natomyndighet för säkerhetsackreditering. I detta fall kan säkerhetsackrediteringen samordnas med den behöriga nationella myndigheten för säkerhetsackreditering.

13.7. Natomyndighet för säkerhetsackreditering (SAA)

13.7.1. För säkerhetsackreditering av Natos kommunikations- och informationssystem (CIS) där Natos säkerhetsskyddsklassificerade information hanteras svarar tre Natomyndigheter för säkerhetsackreditering. Natomyndigheten för säkerhetsackreditering består av chefen för Natos säkerhetsbyrå och de strategiska befälvarna eller deras beordrade eller utsedda företrädare, beroende av vilket kommunikations- och informationssystem som ska ackrediteras.

13.7.2. Natos styrgrupp för säkerhetsackreditering av kommunikations- och informationssystem (NSAB), som består av Natos myndigheter för säkerhetsackreditering (SAA(s)) som anges i punkten ovan, ska för att säkerställa ett gemensamt och konsekvent förhållningssätt till säkerheten för systemen utöva tillsyn över säkerhetsackrediteringen av alla Natos kommunikations- och informationssystem (CIS) där Natos säkerhetsskyddsklassificerade information hanteras. Styrgruppens arbetsordning ska godkännas av säkerhetskommittén.

13.8. Säkerhetsmyndighet i stater utanför Nato (NNN)

13.8.1. En stat utanför Nato (NNN) ska utse en säkerhetsmyndighet som ska ansvara för följandet av säkerhetsbestämmelserna enligt denna bilaga och tillsynen av sådana myndigheter i den staten och som har särskilt ansvar för säkerheten i nationella kommunikations- och informationssystem (CIS Security) där Natos säkerhetsskyddsklassificerade information hanteras (inklusive den nationella säkerhetsmyndigheten för kommunikations- och informationssystem (NCSA), den nationella distributionsmyndigheten (NDA) och myndigheter för säkerhetsackreditering (SAA(s))).

the security accreditation may be co-ordinated with the appropriate national security accreditation authority.

13.7. NATO Security Accreditation Authority (SAA)

13.7.1. There are three NATO SAAs which are responsible for the security accreditation of NATO CIS handling NATO classified information. The SAA shall be the Director, NATO Office of Security and the Strategic Commanders, or their delegated / nominated representative(s), dependent upon the CIS to be accredited.

13.7.2. The NATO CIS Security Accreditation Board, composed of the NATO SAAs as identified in the paragraph above, shall have security accreditation oversight for all NATO CIS handling NATO classified information to ensure a corporate and consistent approach to security of NATO CIS. The NSAB Terms of Reference shall be subject to approval by the Security Committee.

13.8. Security Authority for NNN

13.8.1. The NNN shall appoint a security authority to be responsible for the security provisions of the present Enclosure and the oversight of the NNN Authorities with specific CIS Security responsibilities for national CIS handling NATO classified information (including NCSA, NDA and SAAs).

BILAGA G
C-M(2002)49-REV1

ENCLOSURE "G"
C-M(2002)49-REV1

**BILAGA G
SÄKERHETSSKYDDSKLASSIFICE-
RADE PROJEKT OCH INDUSTRI-
SÄKERHET**

**ENCLOSURE "G"
CLASSIFIED PROJECT AND INDUS-
TRIAL SECURITY**

INLEDNING

1. I denna bilaga presenteras strategin och miniminormerna för säkerheten för Natos säkerhetsskyddsklassificerade information inom industrin. Ytterligare detaljer och krav finns i det stödande direktivet om säkerhetsskyddsklassificerade projekt och industrisäkerhet.

2. Industrisäkerhet är genomförande av skyddsåtgärder och tillämpning av skyddsförfaranden för att förhindra, upptäcka och avhjälpa förlust eller läcka av säkerhetsskyddsklassificerad information som hantearats av industrin inom ramen för kontrakt. Natos säkerhetsskyddsklassificerade information som ges till industrin eller som framställts på grundval av kontrakt som slutits med industrin samt säkerhetsskyddsklassificerade kontrakt som slutits med industrin ska skyddas i enlighet med Natos säkerhetsstrategi och stödande direktiv.

3. De nationella säkerhetsmyndigheterna eller de utsedda säkerhetsmyndigheterna ska säkerställa att de har de medel som krävs för att göra sina krav som gäller industrisäkerhet bindande för industrin och att de har rätt att inspektera och godkänna de åtgärder som genomförts inom industrin för att skydda säkerhetsskyddsklassificerad information.

SÄKERHETSKRAV FÖR VERKSAMHETSSTÄLLEN

4. Alla entreprenörer eller underentreprenörer som sluter kontrakt som inbegriper Natos säkerhetsskyddsklassificerade information och som förutsätter åtkomst till eller framställande av information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller högre ska vid en säkerhetsprövning av verksamhetsställe (FSC) ha beviljats godkänt av den ansvariga nationella

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for the security of NATO Classified Information within industry. Additional details and requirements are found in the supporting Directive on Classified Project and Industrial Security.

2. Industrial security is the application of protective measures and procedures to prevent, detect and recover from the loss or compromise of classified information handled by industry in contracts. NATO Classified Information disseminated to industry, generated as a result of a contract with industry, and classified contracts with industry shall be protected in accordance with NATO Security Policy and supporting directives.

3. NSAs/DSAs shall ensure that they have the means to make their industrial security requirements binding upon industry and that they have the right to inspect and approve the measures taken in industry for the protection of classified information.

FACILITY SECURITY REQUIREMENTS

4. All Contractors/Sub-contractors undertaking a contract involving NATO Classified Information requiring access to, or generation of information classified NATO CONFIDENTIAL (NC) or above shall hold a Facility Security Clearance (FSC) at the appropriate level issued by the responsible NSA/DSA of the country that has jurisdiction over the Contractor/Sub-contractor's

säkerhetsmyndigheten eller den ansvariga utsedda säkerhetsmyndigheten i det land vars jurisdiktion entreprenörens eller underentreprenörens verksamhetsställe omfattas av.

5. En godkänd säkerhetsprövning av verksamhetsställe (FSC) krävs inte för åtkomst till eller framställning av information som säkerhetsskyddsklassificerats som NATO RESTRICTED.

ANBU DS FÖRFARANDE, FÖRHANDLING OCH SLUTANDE AV KONTRAKT SOM INBEGRIPER NATOS SÄKERHETSSKYDDSKLASSIFICERADE INFORMATION

6. Huvudkontraktet för ett Natoprogram eller Natoprojekt ska förhandlas fram och slutas av ett Natoprograms eller Natoprojekts direktion/kontor. Alla entreprenörer som är parter i kontrakt till följd av vilka det vid entreprenörens verksamhetsställe krävs hantering och framställning av eller åtkomst till information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller högre ska ha beviljats godkänt vid en säkerhetsprövning av verksamhetsställe (FSC). För kontrakt som säkerhetsskyddsklassificerats som NATO RESTRICTED krävs inte en godkänd säkerhetsprövning av verksamhetsställe (FSC).

7. Natoprogrammets eller Natoprojektets direktion/kontor eller någon annan kontraktsslutande myndighet som inleder ett kontraktsförfarande ska se till att entreprenörens verksamhetsställen har godkänts vid en adekvat säkerhetsprövning av verksamhetsställe (FSC) när det gäller den specifika fasen av kontraktet. Den kontraktsslutande myndigheten ska kontrollera att entreprenörens personal som i den upphandlande myndighetens lokaler och utrymmen har åtkomst till information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller högre har beviljats godkänt vid en adekvat säkerhetsprövning av person (PSC).

facility.

5. A FSC is not required for access to, or generation of information classified NATO RESTRICTED (NR).

TENDERING, NEGOTIATION AND LETTING OF CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION

6. The prime contract for a NATO programme/project shall be negotiated and awarded by a NATO Programme/Project Agency/Office (NPA/NPO). An FSC shall be required for all Contractors involved in contracts that require the Contractor's facility to manage, generate or have access to information classified NATO CONFIDENTIAL (NC) and above. For contracts classified NATO RESTRICTED (NR), an FSC is not required.

7. The NPA/NPO or other contracting authority which initiates the contract shall ensure that Contractor's facilities hold an appropriate FSC for the specific phase of the contract. The contracting authority shall verify that Contractor's personnel accessing information classified NC or above at the premises of the contracting authority hold the appropriate PSC.

8. Efter det att huvudkontraktet har slutits får en huvudentreprenör förhandla om underkontrakt med andra entreprenörer, det vill säga underentreprenörer. Dessa underentreprenörer får också förhandla om underkontrakt med andra underentreprenörer. Om dessa underkontrakt kräver åtkomst till information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller högre, ska de säkerhetskrav för verksamhetsstället och personalen som anges i avsnittet "Industri säkerhetsgodkännande för Natokontrakt" i denna bilaga och i direktivet om säkerhetsskyddsklassificerade projekt och industri säkerhet gälla. Om en potentiell underentreprenör omfattas av jurisdiktionen¹ för en stat utanför Nato, ska ett förhandstillstånd för förhandling om ett underkontrakt erhållas från Natoprogrammets eller Nato-projektets direktion/kontor eller någon annan kontraktsslutande myndighet. Om Nato-programmet eller Natoprojektet har infört restriktioner för slutandet av kontrakt i de medlemsstater i Nato som inte deltar i programmet eller projektet, lämnas till Natoprogrammet eller Natoprojektet en begäran om att överväga givande av tillstånd och givande av tillstånd innan förhandlingar om kontrakt inleds med entreprenörer från dessa stater.

9. Efter att ha slutit ett kontrakt ska Nato-programmet eller Natoprojektet eller någon annan kontraktsslutande myndighet informera entreprenörens nationella säkerhetsmyndighet eller utsedda säkerhetsmyndighet om kontraktet och säkerställa att tilläggs-klausulen om säkerhet (SAL) och/eller säkerhetsanvisningarna för program/projekt (PSI) i tillämpliga fall tillhandahålls huvudentreprenören tillsammans med kontraktet.

SÄKERHETSKRAV FÖR KONTRAKT SOM INBEGRIPER NATOS SÄKERHETSSKYDDSKLASSIFICERADE INFORMATION

10. Huvudentreprenören och underentreprenörerna ska genom kontrakt åläggas att med

8. After the prime contract has been let, a prime Contractor may negotiate sub-contracts with other Contractors, i.e., Sub-contractors. These Sub-contractors may also negotiate sub-contracts with other Sub-contractors. If these sub-contracts require access to information classified NC and above, the facility and personnel security requirements identified in the "Industrial Security Clearances for NATO Contracts" section of this Enclosure and in the Directive on Classified Project and Industrial Security shall apply. If a potential Sub-contractor is under the jurisdiction¹ of a non-NATO nation prior permission to negotiate a sub-contract shall be obtained from the NPA/NPO or other contracting authority respectively. If the NPA/NPO has placed restrictions on the award of contracts to NATO Nations that are not participants in a programme/project, the NPA/NPO shall be requested to consider and give permission prior to contract discussion with contractors from those Nations.

9. Upon letting the contract, the NPA/NPO or other contracting authority shall notify the NSA/DSA of the Contractor, and ensure that the Security Aspect Letter (SAL) and/or the Project Security Instruction (PSI), as applicable, is provided to the prime Contractor, with the contract.

SECURITY REQUIREMENTS FOR CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION

10. The prime Contractor and Sub-contractors shall be contractually required, under

¹ Rätt att utöva makt i ett visst ärende eller inom ett visst territorium/geografiskt område.

¹ Power to exercise authority over a subject matter or a territory/geographic area.

hot om uppsägning av kontraktet vidta alla åtgärder som föreskrivits av de nationella säkerhetsmyndigheterna eller de utsedda säkerhetsmyndigheterna för skydd av Natos säkerhetsskyddsklassificerade information som framställts av eller anförtros entreprenören, eller som ingår i varor som tillverkats av entreprenören.

a) Till kontrakt för viktiga program/projekt som inbegriper Natos säkerhetsskyddsklassificerade information ska säkerhetsanvisningar för program/projekt (PSI) bifogas; en säkerhetsskyddsklassificeringshandledning för program/projekt ska ingå i säkerhetsanvisningarna för program/projekt. Alla andra kontrakt som inbegriper Natos säkerhetsskyddsklassificerade information ska åtminstone omfatta en tilläggs klausul om säkerhet (SAL), som kan utgöras av säkerhetsanvisningarna för program/projekt men med begränsat tillämpningsområde. I det senare nämnda fallet kan säkerhetsskyddsklassificeringshandledningen för program/projekt kallas en minneslista för säkerhetsskyddsklassificering. Säkerhetsanvisningarna för program/projekt kompletterar Natos säkerhetsstrategi och säkerhetskrav, och i säkerhetsanvisningarna fastställs särskilda säkerhetsförfaranden med anknytning till det berörda Natoprogrammet eller Nato-projektet samt ansvaret för genomförande av säkerhetsåtgärder när det gäller säkerhetsskyddsklassificerad information.

b) För kontrakt som endast omfattar information som säkerhetsskyddsklassificerats som NATO RESTRICTED har det i direktivet om säkerhetsskyddsklassificerade projekt och industrisäkerhet fastställts specifika bestämmelser, särskilt i dess bilaga 4 om kontraktsklausuler om säkerhet i anbud och kontrakt som inbegriper information som säkerhetsskyddsklassificerats som NATO RESTRICTED.

11. Säkerhetsskyddsklassificeringen för program/projekt med information som hänger samman med eventuella underkontrakt ska baseras på säkerhetsskyddsklassificeringshandledningen för program/projekt.

penalty of termination of their contract, to take all measures prescribed by the NSAs/DSAs for protecting all NATO Classified Information generated by or entrusted to the Contractor, or embodied in articles manufactured by the Contractor:

(a) Contracts for major programme/projects involving NATO Classified Information shall contain a PSI as an annex; a "Project Security Classification Guide" shall be a part of the PSI. All other contracts involving NATO Classified Information shall include, as a minimum, a SAL, which may be a PSI that is reduced in scope. In the latter case, the Programme/Project Security Classification Guide may be referred to as a "Security Classification Checklist". The PSI supplements the NATO security policies and requirements, establishes specific security procedures associated with the NATO programme/project concerned and assigns responsibilities for the implementation of security measures concerning classified information.

(b) For contracts involving only information classified NR specific regulations have been established in the Directive on Classified Project and Industrial Security, in particular in its Appendix 4 "Contract Security Clause for Tenders and Contracts involving NATO RESTRICTED Information".

11. The security classification for programme/project elements of information associated with possible sub-contracts shall be based on the Programme/Project Security Classification Guide.

SLUTANDE AV KONTRAKT SOM INBEGRIPER NATOS SÄKERHETS-SKYDDSKLASSIFICERADE INFORMATION MED ENTREPRENÖRER I STATER UTANFÖR NATO

12. När kontrakt som inbegriper Natos säkerhetsskyddsklassificerade information sluts med entreprenörer i stater utanför Nato innebär detta utlämnande av information, vilket ska ske i enlighet med bilaga E till denna C-M-handling, direktivet om säkerhet för Natos säkerhetsskyddsklassificerade information och direktivet om säkerhetsskyddsklassificerade projekt och industri-säkerhet. Utlämnandet ska alltid ske med samtycke av den eller de som informationen härrör från.

13. Slutande av kontrakt som inbegriper Natos säkerhetsskyddsklassificerade information med entreprenörer i stater utanför Nato förutsätter ett bilateralt säkerhetsavtal/säkerhetsarrangemang mellan Nato eller en kontraktsslutande eller som garant fungerande medlemsstat i Nato och en stat utanför Nato. Om kontraktet regleras av ett bilateralt säkerhetsavtal/säkerhetsarrangemang mellan en kontraktsslutande/som garant fungerande medlemsstat i Nato och en stat utanför Nato, ska Natos medlemsstat lämna en skriftlig säkerhetsgaranti till Nato som bekräftelse på att Natos säkerhetsskyddsklassificerade information som lämnas ut omfattas av säkerhetsavtalet/säkerhetsarrangemanget. En kopia av garantin ska lämnas till Natos säkerhetsbyrå och vederbörande Natoprogram eller Natoprojekt.

14. Att sluta ett kontrakt med en entreprenör från en stat utanför Nato ska följa de förfaranden som fastställs i direktivet om säkerhetsskyddsklassificerade projekt och industrisäkerhet.

15. För stater utanför Nato ska en eller flera säkerhetsmyndigheter som sköter motsvarande uppgifter som en nationell säkerhetsmyndighet eller en utsedd säkerhetsmyndighet i en medlemsstat i Nato utses.

CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION WITH CONTRACTORS IN NON-NATO NATIONS

12. The letting of contracts involving NATO Classified Information with Contractors in non-NATO nations constitutes release of information and shall be in accordance with Enclosure "E" to this C-M, the Directive on the Security of NATO Classified Information and the Directive on Classified Project and Industrial Security. The release shall always be with the consent of the relevant originator(s).

13. Contracts involving NATO Classified Information with Contractors in non-NATO nations require the existence of a bilateral Security Agreement/Arrangement between NATO or a contracting/sponsoring NATO Nation and the non-NATO nation. If the contract is governed by a bilateral Security Agreement/Arrangement between a contracting/sponsoring NATO Nation and a non-NATO nation, the NATO Nation shall provide a written Security Assurance to NATO confirming that the NATO Classified Information provided is governed under the scope of that Security Agreement/Arrangement. A copy of the assurance shall be provided to the NOS and the relevant NPO/NPA.

14. Placing a contract to a Contractor of a non-NATO nation shall follow the procedures as established in the Directive on Classified Project and Industrial Security.

15. For non-NATO nations, an appropriate security authority(s) shall be identified that fulfils the equivalent functions of a NATO Nation's NSA/DSA.

SÄKERHETSPRÖVNING INOM INDUSTRIEN NÄR DET GÄLLER NATO-KONTRAKT

Allmänt

16. På kontrakt och underkontrakt tillämpas de principer för verksamhetsställen och personer som beskrivs nedan.

Godkänd säkerhetsprövning av verksamhetsställe (FSC)

17. Den nationella säkerhetsmyndigheten eller den utsedda säkerhetsmyndigheten i varje medlemsstat i Nato ansvarar för att säkerställa att varje verksamhetsställe under dess jurisdiktion som behöver åtkomst till information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller högre har genomfört de säkerhetsskyddsåtgärder som behövs för att kunna beviljas godkänt vid en säkerhetsprövning av verksamhetsställe (FSC). När godkänt beviljas vid en säkerhetsprövning av verksamhetsställe ska den nationella säkerhetsmyndigheten eller den utsedda säkerhetsmyndigheten säkerställa att den har de medel som krävs för att få kännedom om alla omständigheter som kan påverka beviljandet av ett godkännande.

18. Den bedömning som görs innan godkänt beviljas vid en säkerhetsprövning av verksamhetsställe (FSC) ska utöver tillämpliga nationella lagar och regler följa de krav och kriterier som fastställs i det stödjande direktivet om säkerhetsskyddsklassificerade projekt och industrisäkerhet. Bedömningen ska åtminstone inbegripa entreprenörens/underentreprenörens ärlighet och redlighet, säkerhetsstatusen för entreprenörens/underentreprenörens personal och andra personer som på grund av sina förbindelser kan behöva tillgång till Natos säkerhetsskyddsklassificerade information samt utländskt ägande, kontroll och bestämmande inflytande.

19. En anbudsgivare som inte har genomgått en adekvat säkerhetsprövning av verksamhetsställe (FSC) i enlighet med kraven i det potentiella kontraktet/underkontraktet ska inte automatiskt uteslutas ur förfarandet.

INDUSTRIAL SECURITY CLEARANCES FOR NATO CONTRACTS

General

16. The policy described in subsequent paragraphs for facilities and individuals apply to contracts and sub-contracts.

Facility Security Clearances (FSC)

17. The NSA/DSA of each NATO Nation is responsible for ensuring that any facility under its jurisdiction which will require access to information classified NC and above has adopted the protective security measures necessary to qualify for an FSC. In granting an FSC, the NSA/DSA shall ensure that they have the means to be advised of any circumstances that could have a bearing upon the viability of the clearance granted.

18. The assessment to be made prior to issuing an FSC shall be in accordance with the requirements and criteria set out in the supporting Directive on Classified Project and Industrial Security in addition to any applicable national laws and regulations. As a minimum the assessment shall cover aspects of the integrity and probity of the Contractor/Sub-Contractor, security status of its personnel and of other individuals who may, by virtue of their association be required to have access to NATO Classified Information, and aspects of the foreign ownership, control and influence.

19. A bidder, not holding an appropriate FSC as required by the potential contract/subcontract shall not be automatically excluded from the competition. The contract-

Den kontraktsslutande myndigheten ska sträva efter att på alla möjliga sätt se till att den information som lämnas till anbudsgivarna är begränsad till lägsta möjliga säkerhetsskyddsklassificeringsnivå som fortfarande möjliggör ett informationsbaserat och konkurrenskraftigt svar på anbudsinfordran. I anbudsinfordran ska det dock nämnas att godkänt vid en adekvat säkerhetsprövning av verksamhetsställe (FSC) krävs före slutande av kontraktet/underkontraktet.

20. I det stödjande direktivet om säkerhetsskyddsklassificerade projekt och industrisäkerhet anges situationer där en godkänd säkerhetsprövning av verksamhetsställe (FSC) krävs.

21. En godkänd säkerhetsprövning av verksamhetsställe (FSC) eller en godkänd säkerhetsprövning av person (PSC) krävs inte för kontrakt eller åtkomst till information som säkerhetsskyddsklassificerats som NATO RESTRICTED. En stat som enligt sina nationella lagar och regler om säkerhet kräver en godkänd säkerhetsprövning av verksamhetsställe (FSC) för ett kontrakt eller underkontrakt som säkerhetsskyddsklassificerats som NATO RESTRICTED ska inte diskriminera entreprenörer från en stat som inte kräver en godkänd säkerhetsprövning av verksamhetsställe, utan ska säkerställa att entreprenören har informerats om sitt ansvar för skydd av informationen och att denne intygar sig vara medveten om detta ansvar.

Säkerhetsprövning av person för anställda vid verksamhetsställen

22. De anställda vid ett verksamhetsställe som behöver åtkomst till Natos säkerhetsskyddsklassificerade information som säkerhetsskyddsklassificerats som NATO CLASSIFIED eller högre ska ha beviljats godkänt vid en adekvat säkerhetsprövning av person (PSC). Beviljandet av godkänt vid säkerhetsprövning av person ska ske i enlighet med bilaga C till denna C-M-handling, direktivet om personalsäkerhet och direktivet om säkerhetsskyddsklassificerade projekt och industrisäkerhet.

ing authority should make all efforts in restricting the security classification level of the information required to be provided to bidders to the lowest possible level still permitting an informed and qualified response to the invitation to tender. However, the tender document shall advise on the requirement for an appropriate FSC prior to the award of the contract/subcontract.

20. Scenarios identifying FSC requirements are provided in the supporting Directive on Classified Project and Industrial Security.

21. An FSC or PSC is not required for contracts or access to information classified NR. A nation which, under its national security laws and regulations, requires an FSC for a contract or sub-contract classified NR shall not discriminate against a Contractor from a nation not requiring an FSC, but shall ensure that the Contractor has been informed of its responsibilities in respect to the protection of the information, and obtains an acknowledgement of those responsibilities.

Personnel Security Clearances for Facility Employees

22. The facility's employees who require access to NATO Classified Information NC and above shall hold an appropriate PSC. The issuing of PSCs shall be in accordance with Enclosure "C" to this C-M, the Directive on Personnel Security and the Directive on Classified Project and Industrial Security.

23. Ansökningar om säkerhetsprövning av entreprenörers anställda ska lämnas till den nationella säkerhetsmyndighet eller den utsedda säkerhetsmyndighet som ansvarar för verksamhetsstället.

24. Om ett verksamhetsställe vill anställa en medborgare från en stat utanför Nato för en uppgift som förutsätter åtkomst till Natos säkerhetsskyddsklassificerade information, är det den nationella säkerhetsmyndighet eller den utsedda säkerhetsmyndighet under vars jurisdiktion verksamhetsstället i fråga lyder som ska genomföra det förfarande för säkerhetsprövning som fastställs i denna handling och bestämma om personen kan beviljas åtkomst i enlighet med kraven i bilaga C till denna C-M-handling, direktivet om personalsäkerhet och direktivet om säkerhetsskyddsklassificerade projekt och industrisäkerhet.

UTLÄMNANDE AV NATOS SÄKERHETSSKYDDSKLASSIFICERADE INFORMATION VID SLUTANDE AV KONTRAKT

25. Vid slutande av kontrakt kan Natos säkerhetsskyddsklassificerade information lämnas ut antingen till stater utanför Nato och internationella organisationer eller till sådana deltagare från medlemsstater i Nato som inte deltar i program eller projekt. Utlämnandet ska i tillämpliga fall ske med samtycke av det vederbörande Natoprogrammets eller Natoprojektets direktion/kontor och/eller den som informationen härrör från samt i enlighet med andra tillämpliga bilagor till Natos säkerhetsstrategi, direktivet om säkerhet för Natos säkerhetsskyddsklassificerade information och direktivet om säkerhetsskyddsklassificerade projekt och industrisäkerhet.

HANTERING AV SÄKERHETSSKYDDSKLASSIFICERAD INFORMATION I KOMMUNIKATIONS- OCH INFORMATIONSSYSTEM

26. Endast adekvat säkerhetsackrediterade kommunikations- och informationssystem får användas för lagring, bearbetning eller

23. Applications for the security clearance for Contractor employees shall be made to the NSA/DSA which is responsible for the facility.

24. If a facility wishes to employ a citizen of a non-NATO nation in a position that requires access to NATO Classified Information, it is the responsibility of the NSA/DSA of the Nation which has jurisdiction over the hiring facility, to carry out the security clearance procedure prescribed herein, and determine that the individual can be granted access in accordance with the requirements of Enclosure "C" to this C-M, the Directive on Personnel Security and the Directive on Classified Project and Industrial Security.

RELEASE OF NATO CLASSIFIED INFORMATION IN CONTRACTING

25. The release of NATO Classified Information in contracting can constitute either release to non-NATO nations and International Organizations or release to non-Programme/Project participants from NATO Nations. The release shall be with the consent of the relevant NPA/NPO and/or originator, as applicable, and in accordance with other relevant enclosures to the NATO Security Policy, the Directive on the Security of NATO Classified Information as well as the Directive on Classified Project and Industrial Security.

THE HANDLING OF CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)

26. Only appropriately security accredited CIS shall be used for the storing, processing or transmitting (called hereafter "handling") of NATO Classified Information. Enclosure

överföring (nedan hantering) av Natos säkerhetsskyddsklassificerade information. Bilaga F till denna C-M-handling, det primära direktivet om säkerhet i kommunikations- och informationssystem (AC/35-D/2004), direktivet om ledningen av säkerhet i kommunikations- och informationssystem (AC/35-D/2005) och alla adekvata tekniska direktiv och genomförandedirektiv om säkerhet i kommunikations- och informationssystem (AC/322-handlingar) innehåller ytterligare strategier och anvisningar för genomförande av kommunikations- och informationssystem där Natos säkerhetsskyddsklassificerade information hanteras.

27. Säkerhetsackrediteringen av information som säkerhetsskyddsklassificerats som NATO RESTRICTED och som hanteras i kommunikations- och informationssystem kan delegeras till entreprenörer i enlighet med nationella lagar och regler om säkerhet. Om uppgiften delegeras, ska de vederbörande nationella säkerhetsmyndigheterna eller de vederbörande utsedda säkerhetsmyndigheterna eller ackrediteringsmyndigheterna behålla ansvaret för skyddet av information som säkerhetsskyddsklassificerats som NATO RESTRICTED och som hanteras av entreprenören, och de ska ha rätt att inspektera de säkerhetsåtgärder som entreprenörerna genomför.

KONTROLLFÖRFARANDEN VID INTERNATIONELLA BESÖK

28. Kontrollförfaranden vid internationella besök tillämpas på sådana internationella besök som görs av företrädare för Natos medlemsstater, Natos civila och militära organ, entreprenörer och underentreprenörer och som inbegriper Natos säkerhetsskyddsklassificerade information. Kontrollförfarandena tillämpas även på företrädare för stater utanför Nato, inklusive entreprenörer/underentreprenörer från sådana stater, om staten i fråga har godkänt förfarandena.

29. Besök som inbegriper åtkomst till information som säkerhetsskyddsklassificerats som NATO CLASSIFIED eller högre eller obehodsagat tillträde till säkerhetsutrymmen

“F” to this C-M, the “Primary Directive on CIS Security” (AC/35-D/2004), the “Management Directive on CIS security” (AC/35-D/2005) and all relevant Technical and Implementation Directives on CIS Security (AC/322 documents) provide further policy and directions for the conformant implementation of CIS handling NATO Classified Information.

27. The security accreditation of CIS handling information classified NR may be delegated to Contractors according to national security laws and regulations. Where this delegation is exercised, the relevant NSAs/DSAs/SAsAs shall retain the responsibility for the protection of NR information handled by the Contractor and the right to inspect the security measures taken by the Contractors.

INTERNATIONAL VISIT CONTROL PROCEDURES (IVCP)

28. IVCP apply to international visits by representatives of NATO Nations, NATO Civil and Military bodies, Contractors and Sub-Contractors involving NATO Classified Information. They also apply to representatives of a non-NATO nation including Contractors/Sub-Contractors of such Nation if the Nation has adopted the IVCP.

29. Visits involving access to information classified NC and above or unescorted access to security areas shall be approved by the NSA/DSA. Visits involving access to

ska godkännas av den nationella säkerhetsmyndigheten eller den utsedda säkerhetsmyndigheten. Besök som inbegriper åtkomst till information som säkerhetsskyddsklassificerats som NATO UNCLASSIFIED² eller NATO RESTRICTED får anordnas direkt mellan det sändande och det mottagande verksamhetsstället utan formella krav.

30. Detaljerade arrangemang för genomförande av internationella besök fastställs i direktivet om säkerhetsskyddsklassificerade projekt och industrisäkerhet.

PERSONAL SOM LÅNAS UT TILL NATOPROJEKT ELLER NATOPROGRAM

31. När en person, som vid säkerhetsprövning har godkänts för åtkomst till Natos säkerhetsskyddsklassificerade information, i samma Natoprogram eller Natoprojekt lånas ut från ett verksamhetsställe till ett annat i en annan av Natos medlemsstater, ska personens eget verksamhetsställe begära att dess nationella säkerhetsmyndighet eller dess utsedda säkerhetsmyndighet bekräftar för den nationella säkerhetsmyndigheten eller den utsedda säkerhetsmyndigheten för det verksamhetsställe till vilket personen lånas ut att personen är godkänd vid säkerhetsprövning.

INTERNATIONELL ÖVERFÖRING OCH TRANSPORT AV NATOS SÄKERHETSSKYDDSKLASSIFICERADE MATERIAL

På alla transportformer tillämpliga säkerhetsprinciper

32. Vid granskning av de säkerhetsarrangemang som föreslås för internationella transporter av försändelser av säkerhetsskyddsklassificerat material ska följande principer tillämpas:

NU² or information classified NR may be arranged directly between the sending and receiving facility without formal requirements.

30. Detailed arrangements for the conduct of International Visits are laid down in the Directive on Classified Project and Industrial Security.

PERSONNEL ON LOAN WITHIN A NATO PROJECT/ PROGRAMME

31. When an individual who has been cleared for access to NATO Classified Information is to be loaned from one facility to another in the same NATO programme/project, but in a different NATO Nation, the individual's parent facility shall request its NSA/DSA to provide a Personnel Security Clearance Confirmation for the individual to the NSA/DSA of the facility to which they are to be loaned.

INTERNATIONAL TRANSMISSION AND TRANSPORTATION OF NATO CLASSIFIED MATERIAL

Security Principles Applicable to all Forms of Transportation

32. The following principles shall be enforced when examining proposed security arrangements for the international transportation of consignments of classified material:

² NATO UNCLASSIFIED är inte en säkerhetsskyddsklassificering i Nato.

² NU is not a NATO security classification.

a) Säkerheten ska garanteras i alla skeden av transporten och under alla omständigheter från ursprungsplatsen till slutdestinationen.

b) Den skyddsnivå som ges en försändelse ska vara den högsta säkerhetsskyddsklassificeringsnivån för det material som leveransen innehåller.

c) En godkänd säkerhetsprövning av verksamhetsställe (FSC) ska när detta krävs inhämtas för företag som sköter transporten. I sådana fall ska den personal som sköter försändelsen beviljas godkänt vid säkerhetsprövning av person (PSC) i enlighet med bestämmelserna i denna bilaga.

d) Resorna ska i möjligaste mån ske utan omvägar och slutföras så snabbt som omständigheterna medger.

e) Transportrutterna ska noggrant ordnas så att de endast går genom Natos medlemsstater. Rutter genom stater utanför Nato ska endast användas om de godkänts av den nationella säkerhetsmyndighet eller den utsedda säkerhetsmyndighet vars jurisdiktion avsändaren omfattas av och om de är i enlighet med det stödjande direktivet om säkerhet för Natos säkerhetsskyddsklassificerade information.

33. Arrangemang för försändelser av säkerhetsskyddsklassificerat material ska fastställas för varje program eller projekt. Dessa arrangemang ska följas för att minimera sannolikheten för obehörig åtkomst till säkerhetsskyddsklassificerat material.

34. Säkerhetsstandarderna för internationell överföring av Natos säkerhetsskyddsklassificerade information finns i det stödjande direktivet om fysisk säkerhet för Natos säkerhetsskyddsklassificerade information. De detaljerade kraven för personligt överlämnande av säkerhetsskyddsklassificerat Nato-material, överlämnande av säkerhetsskyddsklassificerat material med hjälp av kommersiella kurirföretag, säkerhetsvakter eller ledsagare samt transport av sprängämnen, drivmedel eller andra farliga ämnen fastställs i

(a) security shall be assured at all stages during the transportation and under all circumstances, from the point of origin to the ultimate destination;

(b) the degree of protection accorded to a consignment shall be determined by the highest security classification level of material contained within it;

(c) an FSC shall be obtained, where required, for companies providing transportation. In such cases, personnel handling the consignment shall be issued a PSC in compliance with the provisions of this Enclosure;

(d) journeys shall be point-to-point to the extent possible, and shall be completed as quickly as circumstances permit; and

(e) care shall be exercised to arrange routes only through NATO Nations. Routes through non-NATO nations should only be undertaken when authorised by the NSA/ DSA having jurisdiction over the consignor and in accordance with the supporting Directive on the Security of NATO Classified Information.

33. Arrangements for consignments of classified material shall be stipulated for each programme/project. However, such arrangements shall be in force in order to minimize the likelihood of unauthorised access to classified material.

34. The security standards for the international transfer of NATO Classified Information can be found in the supporting Directive on the Security of NATO Classified Information. However, the detailed requirements for the hand carriage of NATO classified material, carriage of classified material by commercial courier companies, security guards and escorts, and the transportation of explosives, propellants or other dangerous substances are set out in the supporting Directive on Classified Project and Industrial Security.

56/2023

det stödjande direktivet om säkerhets-
skyddsklassificerade projekt och industriell
säkerhet.

BILAGA H
C-M(2002)49-REV1

ENCLOSURE "H"
C-M(2002)49-REV1

**BILAGA H
SÄKERHET I FÖRBINDELSERNA
MED ENHETER SOM INTE HÖR TILL
NATO**

**ENCLOSURE "H"
SECURITY IN RELATION TO NON-
NATO ENTITIES**

INLEDNING

1. I denna bilaga fastställs strategin och miniminormerna för skydd av Natos säkerhets- skyddsklassificerade information när den lämnas ut till stater utanför Nato eller andra organ som inte hör till Nato (till exempel internationella organisationer) eller när dessa har åtkomst till den, inklusive personer som företräder sådana stater eller organ (nedan enheter som inte hör till Nato (NNEs)).

2. Delningen av Natos säkerhetsskyddsklassificerade information med enheter som inte hör till Nato (NNEs) ska ske inom ramen för sådant Natosamarbete som godkänts av Nordatlantiska rådet (NAC). Varje begäran om att dela Natos säkerhetsskyddsklassificerade information med enheter som inte hör till Nato utanför sådant samarbete ska från fall till fall övervägas och godkännas av Nordatlantiska rådet eller den myndighet till vilken uppgiften har delegerats. Ytterligare detaljer och krav för skydd av Natos säkerhetsskyddsklassificerade information när den lämnas ut till enheter som inte hör till Nato eller när dessa har åtkomst till den finns i Natos stödjande direktiv om säkerhet i förbindelserna med enheter som inte hör till Nato.

3. Termen de sju staterna utanför Nato (7NNN) avser endast följande länder och deras medborgare: Australien, Finland, Irland, Nya Zeeland, Schweiz, Sverige och Österrike.¹

4. Enheter som inte hör till Nato (NNEs) ska inrätta en behörig säkerhetsmyndighet med

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for the protection of NATO Classified Information to be released to or accessed by non-NATO nations and other non-NATO bodies (e.g. International Organizations) including individuals representing such nations or bodies (hereinafter referred to as non-NATO entities (NNEs)).

2. The sharing of NATO Classified Information with NNEs shall take place in the context of NATO cooperative activities approved by the North Atlantic Council (NAC). Any request to share NATO Classified Information with NNEs outside such cooperative activities shall be considered and approved by the NAC or the appropriate delegated authority on a case-by-case basis. Additional details and requirements for the protection of NATO Classified Information to be released or accessed by NNEs are found in the supporting Directive for NATO on Security in Relation to NNEs.

3. The term 7 Non-NATO Nations (7NNN) refers solely to the following countries and their citizens: Australia, Austria, Finland, Ireland, New Zealand, Sweden and Switzerland.¹

4. NNEs shall establish an appropriate security authority responsible for the security of

¹ Nationella säkerhetsmyndigheter (NSAs) eller utsedda säkerhetsmyndigheter (DSAs) kan föreslå ändringar i förteckningen över länderna för godkännande av säkerhetskommittén.

¹ NSAs/DSAs may propose changes to the list of countries, for approval by the Security Committee.

ansvar för säkerheten för Natos säkerhets- skyddsklassificerade information. Den stöd- jande handlingen om säkerhet i förbindel- serna med Nato för enheter som inte hör till Nato ger de enheter som inte hör till Nato en översikt över de grundläggande principer och miniminormer för säkerhet som ska till- lämpas på skydd och hantering av Natos sä- kerhetsskyddsklassificerade information och på nationella motsvarigheter som utbyts inom ramen för sådant Natosamarbete som godkänts av Nordatlantiska rådet (NAC).

ALLMÄNNA KRAV

5. Delning av Natos säkerhetsskyddsklassi- ficerade information med enheter som inte hör till Nato (NNEs) kan ske inom ramen för

- a) samarbete som godkänts av Nordatlan- tiska rådet (NAC) och där deltagandet för den enhet som inte hör till Nato (NNE) har godkänts av Nordatlantiska rådet,
- b) Natos verksamhet (till exempel pro- gram, projekt, insatser, uppgifter) där del- tagandet för den enhet som inte hör till Nato och karaktären av enhetens engage- mang i en specifik del av verksamheten anses vara till nytta för Nato, eller
- c) bilaterala åtaganden mellan en med- lemsstat i Nato och en enhet som inte hör till Nato, där delning av Natos säkerhets- skyddsklassificerade information med en- heten som inte hör till Nato har fastställts vara till nytta för Nato.

6. Innan Natos säkerhetsskyddsklassifice- rade information delas med en enhet som inte hör till Nato (NNE) ska enheten och Nato ha ingått ett säkerhetsavtal vars ge- nomförande ska certifieras av Natos säker- hetsavtal ska det finnas en säkerhetsgaranti om det politiskt eller operativt är nödvändigt att rättidigt dela Natos säkerhetsskyddsklas- sificerade information till stöd för samarbete som godkänts av Nordatlantiska rådet (NAC) eller, i undantagsfall, utanför sådant samarbete. I Natos stödjande direktiv om sä- kerhet i förbindelserna med enheter som inte

NATO Classified Information. The Support- ing Document for Non-NATO Entities on Security in Relation to NATO provides the NNEs with an overview of the basic princi- ples and minimum standards of security to be applied to the protection and handling of NATO Classified Information, and national equivalents exchanged in the context of NATO cooperative activities approved by the NAC.

GENERAL REQUIREMENTS

5. The sharing of NATO Classified Infor- mation with NNEs may take place in the contexts of:

- (a) NAC-approved cooperative activities where the NNE's participation has been approved by the North Atlantic Council (NAC);
- (b) NATO activities (e.g. programme, project, operation, task) where the NNE's participation and the nature of its engage- ment in a specific aspect of an activity is deemed beneficial to NATO; or
- (c) bilateral engagements between a NATO Nation and an NNE, where shar- ing of NATO Classified Information with an NNE has been determined to be bene- ficial to NATO.

6. Prior to sharing NATO Classified Infor- mation with an NNE, the NNE and NATO shall have entered into a Security Agree- ment, the implementation of which shall be certified by the NATO Office of Security (NOS). In the absence of a Security Agree- ment, a Security Assurance shall be in place where there is a political or operational im- perative to share NATO Classified Infor- mation in a timely manner in support of a NAC-approved cooperative activity or, in exceptional cases, outside such an activity. The supporting Directive for NATO on Se- curity in Relation to NNEs describes de- tailed provisions applicable to sharing

hör till Nato (NNEs) finns detaljerade bestämmelser om delning av Natos säkerhets-skyddsklassificerade information med enheter som inte hör till Nato i de sammanhang som anges i punkt 5.

SÄKERHETSAVTAL OCH ADMINISTRATIVA ARRANGEMANG

7. Ett säkerhetsavtal är en mekanism som används för att göra det möjligt att utbyta säkerhetsskyddsklassificerad information med en identifierad enhet som inte hör till Nato (NNE). Ett säkerhetsavtal innehåller de strategiska principer på hög nivå som överenskommit mellan Nato och en enhet som inte hör till Nato och utgör grunden för genomförandet av lämpliga säkerhetsåtgärder för att vid behov skydda både Natos säkerhetsskyddsklassificerade information och säkerhetsskyddsklassificerad information från den enhet som inte hör till Nato. Genomförandet av säkerhetsavtalet av den enhet som inte hör till Nato ska certifieras av Natos säkerhetsbyrå (NOS) innan Natos säkerhetsskyddsklassificerade information lämnas ut till enheten.

8. De säkerhetsprinciper som fastställs i säkerhetsavtalet ska stödjas av en lämplig uppsättning administrativa arrangemang. De administrativa arrangemangen stöder genomförandet av säkerhetsavtalet och består av en uppsättning bestämmelser som beskriver de grundläggande säkerhetskraven för det adekvata och ömsesidigt godtagbara skyddet av den säkerhetsskyddsklassificerade information som utbyts. När de administrativa arrangemangen har ingåtts bekräftar Natos säkerhetsbyrå (NOS) tillämpningen av dem genom en säkerhetskartläggning.

9. Natos säkerhetsbyrå (NOS) ska med stöd av en riskhanteringsmetod utföra regelbundna säkerhetskartläggningar minst vartannat år i de relevanta organen inom den enhet som inte hör till Nato (NNE) för att säkerställa fortsatt efterlevnad av säkerhetsavtalet och de administrativa arrangemangen.

NATO Classified Information with NNEs in the contexts specified in paragraph 5.

SECURITY AGREEMENTS AND ADMINISTRATIVE ARRANGEMENTS

7. A Security Agreement is a mechanism used to enable the exchange of classified information with an identified NNE. It sets out high level strategic principles agreed between NATO and the NNE, providing the basis for the implementation of appropriate security measures to protect NATO Classified Information as well as the NNE's classified information, when required. The implementation of the Security Agreement by the NNE shall be certified by the NOS before any NATO Classified Information is released to an NNE.

8. The security principles identified in the Security Agreement shall be supported by an appropriate set of Administrative Arrangements. The Administrative Arrangements act in support of the implementation of a Security Agreement and are a set of provisions which outline the basic security requirements for the appropriate and mutually acceptable protection of the exchanged classified information. Once the Administrative Arrangements have been concluded their application shall be confirmed by the NOS through the conduct of a security survey.

9. The NOS shall carry out periodic security surveys, at least once every two years, based on a risk management approach, of the relevant bodies within the NNE to ensure continued compliance with the Security Agreement and the Administrative Arrangements.

SÄKERHETSGARANTIER

10. En säkerhetsgaranti används i avsaknad av ett certifierat säkerhetsavtal mellan Nato och en enhet som inte hör till Nato om det politiskt eller operativt är nödvändigt att rätttidigt dela Natos säkerhetsskyddsklassificerade information till stöd för samarbete som certifierats av Nordatlantiska rådet (NAC) eller, i undantagsfall, utanför sådant samarbete. I Natos stödjande direktiv om säkerhet i förbindelserna med enheter som inte hör till Nato (NNEs) ingår detaljerade kriterier som ska uppfyllas i de fall då en säkerhetsgaranti används.

11. En säkerhetsgaranti formaliserar åtagandet för en enhet som inte hör till Nato (NNE) att tillhandahålla en adekvat nivå av skydd för Natos säkerhetsskyddsklassificerade information som enheten tar emot. En säkerhetsgaranti är begränsad till specifik verksamhet för en bestämd tid.

12. En säkerhetsgaranti från en enhet som inte hör till Nato (NNE), undertecknad av en företrädare som vederbörligen bemyndigats av enheten, ska ges in till Natos säkerhetsbyrå (NOS) i de fall då säkerhetsgarantin används för att göra det möjligt att dela Natos säkerhetsskyddsklassificerade information till stöd för

- a) samarbete godkänt av Nordatlantiska rådet, eller
- b) Natos verksamhet när deltagandet för en enhet som inte hör till Nato (NNE) från fall till fall har godkänts av Nordatlantiska rådet (NAC) eller den myndighet till vilken uppgiften har delegerats.

Garantier från en medlemsstat i Nato

13. Delning av Natos säkerhetsskyddsklassificerade information utanför den verksamhet som definieras i punkt 12 a eller 12 b kräver, efter en särskild begäran från en medlemsstat i Nato, garantier. Garantier innebär en form av stöd från en medlemsstat i Nato till en enhet som inte hör till Nato (NNE) för att göra det möjligt att dela Natos säkerhetsskyddsklassificerade information med en enhet som inte hör till Nato när det inte finns

SECURITY ASSURANCES

10. A Security Assurance is utilized in the absence of a certified Security Agreement between NATO and an NNE where there is a political or operational imperative that necessitates the sharing of NATO Classified Information in a timely manner in support of a NAC-approved cooperative activity, or in exceptional cases outside such an activity. The supporting Directive for NATO on Security in Relation to NNEs provides detailed criteria to be fulfilled in cases when a Security Assurance is used.

11. A Security Assurance formalises the NNE's commitment to provide an appropriate degree of protection to any NATO Classified Information received. A Security Assurance is limited to the specific activity, for a specific period of time.

12. A Security Assurance from an NNE, signed by a representative duly mandated by the NNE, shall be provided to the NOS in cases where a Security Assurance is utilized for the purposes of enabling sharing of NATO Classified Information in support of a:

- (a) NAC-approved cooperative activity, or
- (b) NATO activity, where the NNE's participation has been approved by the NAC or the appropriate delegated authority, on a case-by-case basis.

Sponsorship by a NATO Nation

13. Sharing of NATO Classified Information outside activities defined in 12 (a) or (b), further to a special request by a NATO Nation, requires sponsorship. A sponsorship means a form of support provided by a NATO Nation to an NNE in order to enable sharing of NATO Classified Information with an NNE in case of absence of a certified Security Agreement between NATO and the NNE.

något certifierat säkerhetsavtal mellan Nato och den enheten.

14. För att en medlemsstat i Nato ska kunna vara garant ska det finnas ett lämpligt säkerhetsramverk (till exempel ett säkerhetsavtal eller något annat tillämpligt arrangemang) mellan garanten och den enhet som inte hör till Nato (NNE). Garanten ska ge in en skriftlig säkerhetsgaranti, undertecknad av en företrädare som vederbörligen bemyndigats av den enhet som inte hör till Nato, till Natos säkerhetsbyrå (NOS). I säkerhetsgarantin fastställs de miniminormer som den enhet som inte hör till Nato ska tillämpa för att skydda Natos säkerhetsskyddsklassificerade information.

15. En garanti är begränsad till specifik verksamhet för en bestämd tid.

SÄRSKILDA SÄKERHETSBESTÄM- MELSER

16. När Natos säkerhetsskyddsklassificerade information delas med enheter som inte hör till Nato (NNEs), finns det tre sätt för att ge åtkomst till Natos säkerhetsskyddsklassificerade information eller tillträde till Natos lokaler och utrymmen till enheter som inte hör till Nato: genom tillträde till Natos lokaler och utrymmen, åtkomst till Natos säkerhetsskyddsklassificerade information och utlämnande av Natos säkerhetsskyddsklassificerade information. I Natos stödjande direktiv om säkerhet i förbindelserna med enheter som inte hör till Nato (NNEs) finns detaljerade kriterier med anslutande specifika åtgärder och förfaranden som är tillämpliga i varje situation.

Personalsäkerhet

17. Innan en person från en enhet som inte hör till Nato (NNE) beviljas åtkomst till information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller högre, ska personen ha beviljats godkänt vid en säkerhetsprövning av person (PSC) på minst samma nivå som krävs för en medborgare i en medlemsstat i Nato i enlighet med Natos säkerhetsstrategi och dess stödjande direktiv.

14. In order for a NATO Nation to be able to act as a Sponsor there shall be an appropriate security framework (e.g. security agreement or other applicable arrangement) in place between the Sponsor and the NNE. The Sponsor shall provide a written Security Assurance, signed by a representative duly mandated by the NNE, to the NOS. The Security Assurance stipulates the minimum standards that the NNE shall apply for the protection of NATO Classified Information.

15. A sponsorship is limited to a specific activity, for a specific period of time.

SPECIFIC SECURITY PROVISIONS

16. When sharing NATO Classified Information with NNEs there are three circumstances in which access to NATO Classified Information or premises can be provided to NNEs: access to NATO premises, access to NATO Classified Information, and release of NATO Classified Information. The supporting Directive for NATO on Security in Relation to NNEs provides detailed criteria and the related specific measures and procedures applicable for each scenario.

Personnel Security

17. Before an NNE individual is granted access to information classified NC or above, the individual shall have successfully completed a PSC procedure no less rigorous than that required for a NATO national in accordance with NATO Security Policy and its supporting directives.

18. En godkänd säkerhetsprövning av person (PSC) krävs inte för åtkomst till information som säkerhetsskyddsklassificerats som NATO RESTRICTED. Personer från en enhet som inte hör till Nato (NNE) ska dock ha behovslenig behörighet, ha informerats om sina säkerhetsåligganden när det gäller skyddet av Natos säkerhetsskyddsklassificerade information och skriftligen eller på ett motsvarande sätt som säkerställer oavvislighet ha intygat att de är medvetna om sitt säkerhetsansvar.

19. En godkänd säkerhetsprövning av person (PSC) kan krävas för tillträde till Natos lokaler och utrymmen på grundval av särskilda kriterier som fastställs i Natos stödjande direktiv om säkerhet i förbindelserna med enheter som inte hör till Nato (NNEs) samt de relevanta lokala säkerhetsbestämmelserna.

Fysisk säkerhet

20. Personer från enheter som inte hör till Nato (NNEs) och som på grund av sitt uppdrag och sin tjänsteutövning behöver ha regelbundna kontakter med Natos personal kan ges tillträde till särskilda utrymmen där information som säkerhetsskyddsklassificerats som NATO RESTRICTED eller högre lagras, hanteras och/eller diskuteras. Sådana personer kan också tilldelas arbetsrum inom särskilda zoner. Beviljande av obeleddat tillträde till och/eller tilldelning av arbetsrum ska behandlas från fall till fall.

21. I Natos stödjande direktiv om säkerhet i förbindelserna med enheter som inte hör till Nato (NNEs) finns detaljerad information om förfarandet, godkännandemyndigheterna och de kriterier som ska uppfyllas för att personer från enheter som inte hör till Nato ska beviljas tillträde till Natos säkerhetsutrymme av klass I eller II eller till en administrativ zon.

18. A PSC is not required for access to information classified NATO RESTRICTED (NR). However, the NNE individual shall have a need-to-know, shall be briefed on their security obligations in respect to the protection of NATO Classified Information and shall have acknowledged their security responsibilities in writing or an equivalent method which ensures non-repudiation.

19. A PSC may be required to access NATO premises based on specific criteria stipulated in the supporting Directive for NATO on Security in Relation to NNEs, and the relevant local security regulations.

Physical Security

20. Individuals from NNEs who, because of their assignment and official duties, need regular interface with NATO staff may be granted access to specific areas in which information classified NR and above is stored, handled and/or discussed. Such individuals may also be assigned office space within specific areas. The granting of unescorted access and/or the assignment of office space shall be handled on a case-by-case basis.

21. The supporting Directive for NATO on Security in Relation to NNEs provides detailed information on the procedure, approval authorities and the criteria to be fulfilled for individuals from NNEs to be granted access to a NATO Class I or Class II Security Area, or to an Administrative Zone.

Informationssäkerhet

22. Inom ramen för samarbete med enheter som inte hör till Nato (NNEs) kan åtkomst till Natos säkerhetsskyddsklassificerade information eller tillträde till Natos lokaler och utrymmen ges på följande tre sätt till enheter som inte hör till Nato:

a) **tillträde till Natos lokaler och utrymmen.** En person som företräder en enhet som inte hör till Nato har tillstånd att fysiskt få tillträde till en viss plats, ett visst verksamhetsställe eller ett visst utrymme i ett verksamhetsställe inom Nato. Fysiskt tillträde innefattar inte automatiskt åtkomst till Natos säkerhetsskyddsklassificerade information.

b) **åtkomst till Natos säkerhetsskyddsklassificerade information.** En person som företräder en enhet som inte hör till Nato har tillstånd att få åtkomst till Natos säkerhetsskyddsklassificerade information för att fullgöra sina uppdrag och sin tjänstutövning, när åtkomsten är till nytta för Nato. Åtkomsten är begränsad till personen i fråga, som inte får sprida Natos säkerhetsskyddsklassificerade information vidare till sin enhet som inte hör till Nato, såvida inte informationen har lämnats ut i enlighet med de fastställda förfarandena.

c) **utlämnande av Natos säkerhetsskyddsklassificerade information.** När Natos säkerhetsskyddsklassificerade information med tillstånd får lämnas ut till en enhet som inte hör till Nato.

23. I Natos stödjande direktiv om säkerhet i förbindelserna med enheter som inte hör till Nato (NNEs) finns detaljerade kriterier som måste uppfyllas när under särskilda omständigheter Natos civila eller militära organ eller Natos medlemsstater ska ge åtkomst till eller lämna ut Natos säkerhetsskyddsklassificerade information.

24. Utlämnande av Natos säkerhetsskyddsklassificerade information till en enhet som inte hör till Nato (NNE) är alltid beroende av ett skriftligt samtycke i förväg av den eller de som informationen härrör från.

Security of Information

22. In the context of cooperation with NNEs there are three circumstances in which access to NATO Classified Information or premises can be provided to NNEs:

(a) **Access to NATO premises.** A circumstance when an individual representing an NNE is authorised to physically access a specific NATO site, facility or specific area located within a facility. Physical access does not automatically include access to NATO Classified Information.

(b) **Access to NATO Classified Information.** A circumstance when an individual representing an NNE is authorised to access NATO Classified Information in order to fulfil their assignments and official duties when access is for NATO's benefit. Access is limited to the individual in question and they are not permitted to disseminate NATO Classified Information further to their NNE unless that information has been released in accordance with the established procedures.

(c) **Release of NATO Classified Information.** A circumstance when NATO Classified Information is authorised to be released to an NNE.

23. The supporting Directive for NATO on Security in Relation to NNEs provides detailed criteria that needs to be fulfilled in specific circumstances when access to or release of NATO Classified Information is to be provided by NATO Civil or Military bodies, or by NATO Nations.

24. Release of NATO Classified Information to an NNE is always subject to receiving prior written consent of the originator(s).

25. Natos säkerhetsskyddsklassificerade information får lämnas ut inom ramen för samarbete som godkänts av Nordatlantiska rådet (NAC) eller inom ramen för Natos verksamhet, om Nordatlantiska rådet eller den myndighet till vilken uppgiften har delegerats har godkänt deltagarna från den enhet som inte hör till Nato (NNE) i verksamheten. I Natos stödande direktiv om säkerhet i förbindelserna med enheter som inte hör till Nato finns detaljerade kriterier som ska tillämpas innan informationen lämnas ut.

26. För att Natos säkerhetsskyddsklassificerade information ska kunna lämnas ut på en särskild begäran av en medlemsstat i Nato (garanten) till en enhet som inte hör till Nato (NNE) utanför sådant samarbete som har godkänts av Nordatlantiska rådet (NAC) eller utanför Natos verksamhet, och där deltagarna från den enhet som inte hör till Nato har godkänts av Nordatlantiska rådet eller den myndighet till vilken uppgiften har delegerats, ska före utlämnandet de ytterligare kriterier som finns i Natos stödande direktiv om säkerhet i förbindelserna med enheter som inte hör till Nato tillämpas.

27. Om ett säkerhetsavtal eller en säkerhetsgaranti är i kraft med en internationell organisation, ska utlämnandet av Natos säkerhetsskyddsklassificerade information till dem i avtalet eller garantin som inte hör till Nato ske i enlighet med de relevanta bestämmelserna i säkerhetsavtalet och andra fastställda regler för deras deltagande i Natos verksamhet. När i avsaknad av ett säkerhetsavtal en säkerhetsgaranti har upprättats med en internationell organisation, ska utlämnandet av Natos säkerhetsskyddsklassificerade information till dem i garantin som inte hör till Nato ske i enlighet med de relevanta bestämmelserna i det stödande direktivet och säkerhetsgarantin.

28. En enhet som inte hör till Nato (NNE) och som inte är part i det gällande avtalet mellan parterna i nordatlantiska fördraget om samarbete avseende nukleär information (C-M(64)39) får inte ha eller ges åtkomst till

25. NATO Classified Information may be released in the context of NAC-approved cooperative activity or in the context of NATO activities, where the NNE participants to that activity have been endorsed by the NAC or the appropriate delegated authority. The supporting Directive for NATO on Security in Relation to NNEs provides additional criteria to be applied prior to release.

26. For NATO Classified Information to be released on a special request from a NATO Nation (the Sponsor) to an NNE outside NAC-approved cooperative activities or NATO activities, where the NNE participants in that activity have been endorsed by the NAC or the appropriate delegated authority, the supporting Directive for NATO on Security in Relation to NNEs provides additional criteria to be applied prior to release.

27. Where a Security Agreement or Security Assurance is in force with an international organization, the release of NATO Classified Information to its non-NATO members shall be in accordance with the relevant provisions of the Security Agreement, as well as other established rules concerning their participation in NATO activities. In the absence of a Security Agreement, where a Security Assurance is in place with an international organization, the release of NATO Classified Information to its non-NATO members shall be in accordance with the relevant provisions of the supporting Directive and the Security Assurance.

28. ATOMAL information of any security classification shall not be accessed by or released to any NNE which is not a party to the current Agreement Between the Parties

Atomalinformation av någon som helst säkerhetsskyddsklassificering.

Utlämnande myndighet

29. Nordatlantiska rådet (NAC) har den högsta befogenheten när det gäller utlämnande av Natos säkerhetsskyddsklassificerade information till enheter som inte hör till Nato (NNEs). Denna befogenhet följer principen om samtycke av den som informationen härrör från och befogenheten delegeras till

a) den lämpliga ämnesspecifika kommittén när det gäller information som säkerhetsskyddsklassificerats som NATO SECRET eller lägre och som härrör från den kommittén och/eller dess underordnande organ. När det gäller information som säkerhetsskyddsklassificerats som NATO RESTRICTED får den lämpliga ämnesspecifika kommittén vidaredelegera befogenheten till en tydligt identifierad funktion inom den stödjande personalen eller till en särskild roll/särskilda roller inom den ämnesspecifika kommitténs stödjande personal,

b) militärkommittén (MC) när det gäller information som säkerhetsskyddsklassificerats som NATO SECRET eller lägre och som härrör från militärkommittén och/eller dess underordnande organ. När det gäller information som säkerhetsskyddsklassificerats som NATO RESTRICTED får militärkommittén vidaredelegera befogenhet till en tydligt identifierad funktion inom den stödjande personalen eller till en särskild roll/särskilda roller inom militärkommitténs stödjande personal,

c) högsta befälhavaren för Natos styrkor i Europa (SACEUR) eller biträdande högsta befälhavaren för Natos styrkor i Europa (D/SACEUR) när det gäller information som säkerhetsskyddsklassificerats som NATO SECRET eller lägre och som det anses att kan lämnas ut till ett visst uppdrag (XFOR) eller som har säkerhetsskyddsklassificerats som NATO/XFOR

to the North Atlantic Treaty for Co-operation Regarding Atomic Information C-M(64)39.

Release Authority

29. The NAC is the ultimate authority for the release of NATO Classified Information to NNEs. This authority respects the principle of originator consent and is delegated to:

(a) the appropriate subject-matter committee for information classified up to and including NS which has been originated by that committee and/or bodies subordinate to it. For information classified NR, the appropriate subject-matter committee may further delegate authority to a clearly identified staff support function or a specific role(s) within the support staff to that committee;

(b) the MC for information classified up to and including NS which has been originated by the MC and/or bodies subordinate to it. For information classified NR, the MC may further delegate authority to a clearly identified staff support function or a specific role(s) within the support staff to the MC;

(c) SACEUR or D/SACEUR for information classified up to and including NS which is identified as being releasable to the mission (XFOR), or is classified NATO/ XFOR SECRET (mission SECRET), under specific conditions, which are in detail described in the supporting Directive for NATO on Security in Relation to NNEs;

SECRET (mission SECRET), på särskilda villkor som beskrivs i detalj i Natos stöd- jande direktiv om säkerhet i förbindel- serna med enheter som inte hör till Nato,

d) befälhavaren över transformationsled- ningen (SACT) eller biträdande befälha- varen över transformationsledningen (D/SACT) när det gäller information som säkerhetsskyddsklassificerats som NATO SECRET eller lägre, på särskilda villkor som beskrivs i detalj i Natos stöd- jande direktiv om säkerhet i förbindel- serna med enheter som inte hör till Nato,

e) uppdragschefen för en insats som inbe- griper truppbidragande stater utanför Nato (NNTCN), i enlighet med godkännande av Nordatlantiska rådet, när det gäller in- formation som säkerhetsskyddsklassifice- rats som NATO SECRET eller lägre och som det redan har fastställts att kan läm- nas ut till uppdraget (XFOR) på särskilda villkor som beskrivs i detalj i Natos stöd- jande direktiv om säkerhet i förbindel- serna med enheter som inte hör till Nato,

f) Natos produktions- och logistikorgani- sation (NPLO), i samordning med de del- tagande staterna, när det gäller Natos sä- kerhetsskyddsklassificerade information som härrör från och tillhör en eller flera av de stater som deltar i Natos produktions- och logistikorganisation.

30. Med hänsyn till de avvikelser som anges i punkterna 29 a och 29 b och som gäller in- formation som säkerhetsskyddsklassificerats som NATO RESTRICTED får de myndig- heter till vilka utlämnandet delegerats inte vidaredelegera sina befogenheter.

31. Utlämnandebefogenheten får endast de- legeras till en lämplig ämnesspecifik kom- mitté där den eller de som informationen härrör från företräds. Om en eller flera av dem som informationen härrör från inte kan fastställas, ska den behöriga ämneskommit- tén överta ansvaret från den som informat- ionen härrör från.

32. I genomförandeinstruktionerna för del- ning av underrättelseinformation mellan

(d) SACT or D/SACT for information classified up to and including NS infor- mation, under specific conditions, which are in detail described in the supporting Directive for NATO on Security in Rela- tion to NNEs;

(e) the mission commander for an opera- tion involving Non-NATO Troop Con- tributing Nations (NNTCN), as endorsed by the NAC, for information classified up to and including NS that has already been determined as releasable to the mission (XFOR), under specific conditions, which are in detail described in the sup- porting Directive for NATO on Security in Relation to NNEs;

(f) the NATO Production and Logistics Organization (NPLO), in coordination with the participating nations, for NATO Classified Information originated by and belonging to one or more of the nations participating in the NPLO.

30. With the exceptions applying to infor- mation classified NR stated in paragraphs 29 (a) and (b) above, delegated release authori- ties cannot further delegate their powers.

31. Authority for release shall only be dele- gated to an appropriate subject-matter com- mittee on which the originator(s) is/are rep- resented. If the originator(s) cannot be es- tablished, the appropriate subject-matter committee shall assume the responsibility of the originator.

32. The Implementing Instructions on Intel- ligence Sharing Between NATO and NNEs

Nato och enheter som inte hör till Nato (NNEs) (DSG (2015) 0307-REV1) och den stödjande handlingen om delning av under rättelseinformation och annan information med enheter som inte hör till Nato (AC/35-D/1040) definieras den utlämnande myndigheten i miljöer som gäller operationer, utbildning, övningar, transformation eller samarbete.

Registrering av utlämnad information

33. Natos civila och militära organ ska föra register över beslut om all information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller högre och som de har lämnat ut till en enhet som inte hör till Nato (NNE) och de ska minst var sjätte månad till Natos centralregister i Bryssel rapportera uppgifter om referensnummer, titel och datum för utlämnande, om inte en behörig säkerhetsmyndighet bestämmer något annat.

Säkerhet i kommunikations- och informationssystem

34. I Natos stödjande direktiv om säkerhet i förbindelserna med enheter som inte hör till Nato (NNEs) anges särskilda krav som ska uppfyllas för att en person från en enhet som inte hör till Nato ska kunna få åtkomst till Natos kommunikations- och informationssystem (CIS).

35. En sammankoppling av Natos kommunikations- och informationssystem (CIS) med ett kommunikations- och informationssystem i en enhet som inte hör till Nato ska vara säkerhetsackrediterad i enlighet med Natos säkerhetsstrategi och dess stödjande direktiv.

SÄKERHETSINCIDENTER

36. En säkerhetsincident som inbegriper säkerhetsskyddsklassificerad information som Nato haft och erhållit från en enhet som inte hör till Nato (NNE) ska följa bestämmelserna i direktivet om säkerhet för Natos säkerhetsskyddsklassificerade information (AC/35-D/2002) och eventuella ytterligare bestämmelser som anges i säkerhetsavtalet

(DSG(2015)0307-REV1) and the Supporting Document on Information and Intelligence Sharing with Non-NATO Entities (AC/35-D/1040) define the Release Authority in the environments of Operations, Training, Exercises, Transformation or Cooperation.

Records of Released Information

33. NATO Civil and Military bodies shall keep records of decisions of all information classified NC and above which they have released to an NNE and shall, at least every six months, report details of the reference number, title and release date to the NATO Central Registry, Brussels, unless otherwise directed by an appropriate Security Authority.

Communication and Information Systems Security

34. The supporting Directive for NATO on Security in Relation to NNEs outlines specific requirements that shall be met in order for an NNE individual to be provided access to NATO Communication and Information System (CIS).

35. Interconnection of NATO CIS with an NNE's CIS shall be security accredited in accordance with the NATO Security Policy and its supporting directives.

SECURITY INCIDENTS

36. Security incidents involving an NNE's classified information in NATO's possession shall follow the provisions of the Directive on the Security of NATO Classified Information (AC/35-D/2002) and any additional provisions specified in the Security

och de administrativa arrangemangen för genomförandet av det eller i säkerhetsgarantin för den enhet som inte hör till Nato.

37. Säkerhetsincidenter som inbegriper säkerhetsskyddsklassificerad information från en enhet som inte hör till Nato (NNE) ska omedelbart rapporteras till Natos säkerhetsbyrå (NOS). Natos säkerhetsbyrå ansvarar för att omgående informera den relevanta säkerhetsmyndigheten för en enhet som inte hör till Nato om säkerhetsincidenter som inbegriper säkerhetsskyddsklassificerad information från enheten som inte hör till Nato i enlighet med säkerhetsavtalet och dess administrativa arrangemang för genomförandet eller säkerhetsgarantin.

Agreement and the implementing Administrative Arrangements, or Security Assurance with the NNE.

37. Security incidents involving an NNE's classified information shall be immediately reported to the NOS. The NOS is responsible for promptly informing the relevant NNE's Security Authority on security incidents involving an NNE's classified information in accordance with the Security Agreement and the implementing Administrative Arrangements, or Security Assurance.

ORDLISTA
C-M(2002)49-REV1

GLOSSARY
C-M(2002)49-REV1

ORDLISTA		GLOSSARY	
Åtkomst till information	Beviljande av tillåtelse för en eller flera personer att ta del av särskild information i enlighet med de säkerhetsbegränsningar som krävs för utförande av deras tydligt definierade uppgifter, för vilka de har tillbörliga befogenheter. Åtkomst till information under sådana omständigheter är den berörda personens privilegium och inbegriper inte rätt att ytterligare sprida informationen.	Access to information	The granting of permission for an individual or individuals to be exposed to specific information in line with the required security parameters for the execution of their clearly defined and appropriately authorized duties. Access in such circumstances is the privilege of the individual in question where rights of further dissemination are not permitted.
Tillträde till lokaler och utrymmen	Beviljande av tillåtelse till fysiskt tillträde till en angiven plats där en eller flera namngivna personer får närvara antingen med eller utan en utsedd ledsagare beroende på vad respektive säkerhetskrav förutsätter och respektive godkänd säkerhetsprövning tillåter.	Access to premises	The granting of permissions for the physical access to a defined location where a nominated individual or individuals will be allowed to be present either with or without a designated escort dependent upon specific security requirements and clearances.
Information som omfattas av ansvarsskyldighet	All information som säkerhetsskyddsklassificerats som COSMIC TOP SECRET (CTS) eller NATO SECRET (NS) samt all information av särskild kategori (såsom ATOMAL).	Accountable Information	All information classified CTS and NS and all Special Category Information. (such as ATOMAL)
Administrativ zon	En tydligt avgränsad skyddad zon där personer inte behöver ledsagas och dit tillträde kräver tillstånd.	Administrative Zone	A clearly defined protected area in which individuals are not required to be escorted and to which access is subject to authorization.

Aggregationsprincipen	När en stor mängd av Natos säkerhetsskyddsklassificerade information samlas ihop måste den ursprungliga säkerhetsskyddsklassificeringsmärkningsmärke bibehållas och en bedömning av hur organisationen påverkas om den samlade informationen går förlorad eller läcker görs. Om denna övergripande effekt bedöms vara större än effekten av Natos berörda enskilda säkerhetsskyddsklassificeringsnivåer, ska hantering och skydd av den samlade informationen på en nivå som motsvarar den bedömda effekten av att den samlade informationen går förlorad eller läcker övervägas.	Aggregation Principle	When a large amount of NATO Classified Information is collated together, the original security classification markings must be retained and that information shall be assessed for the impact its collective loss or compromise would have upon the organization. If this overall impact is assessed as being higher than the impact of the actual individual NATO security classifications then consideration should be given to handling and protecting it at a level commensurate with the assessed impact of its loss or compromise.
Autentisering	Autentisering innebär att en enhets påstådda identitet kontrolleras.	Authentication	Authentication is the act of verifying the claimed identity of an entity.
Tillgänglighet	Informationens och materialets tillgänglighet och användbarhet vid anfordran av en behörig person eller enhet.	Availability	The property of information and material being accessible and usable upon demand by an authorised individual or entity.
Säkerhetsskyddsklassificerad information	All information (det vill säga kunskap som kan överföras i vilken form som helst) eller alla material som kräver skydd mot obehörigt röjande och som med säkerhetsskyddsklassificering har angetts vara sådan.	Classified Information	Any information (namely, knowledge that can be communicated in any form) or material determined to require protection against unauthorised disclosure and which has been so designated by a security classification.

Säkerhet i kommunikations- och informationssystem (CIS Security)	Vidtagande av säkerhetsåtgärder för att skydda kommunikations- och informationssystem och andra elektroniska system samt den information som lagras, behandlas eller överförs i dessa system med avseende på konfidentialitet, riktighet, tillgänglighet, autentisering och oavvislighet.	Communication and Information System Security (CIS Security)	The application of security measures for the protection of communication, information and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.
Behörig säkerhetsmyndighet (CSA)	En myndighet som utses av den nationella säkerhetsmyndigheten och som har behörighet att utföra särskilda säkerhetsuppgifter, inbegripet sådana som gäller beviljande av godkänt vid en säkerhetsprövning av person, för att ge den berörda statens medborgare åtkomst till Natos säkerhetsskyddsklassificerade information.	Competent Security Authority (CSA)	An authority identified by the NSA which is authorised to carry out specific security roles including those relating to personnel security clearances in order to give their nationals access to NATO Classified Information.
Läcka	En läcka innebär en situation där på grund av säkerhetsöverträdelse eller skadlig verksamhet (såsom spionage, terroristhandlingar, sabotage eller stöld) Natos säkerhetsskyddsklassificerade information har förlorat sin konfidentialitet, riktighet eller tillgänglighet eller där de stödjande tjänsterna och resurserna har förlorat sin riktighet eller tillgänglighet. Detta inbegriper förlust, röjande till obehöriga per-	Compromise	Compromise denotes a situation when - due to a Security Breach or adverse activity (such as espionage, acts of terrorism, sabotage or theft) - NATO Classified Information has lost its confidentiality, integrity or availability, or supporting services and resources have lost their integrity or availability. This includes loss, disclosure to unauthorized individuals (e.g. through espionage or to the me-

	soner (till exempel genom spionage eller till medier), otillåtna ändringar, utplåning på otillåtet sätt eller överbelastning.		dia) unauthorized modification, destruction in an unauthorised manner, or denial of service.
Kommunikations-center	En organisation som ansvarar för hantering och kontroll av kommunikationstrafik och som vanligtvis består av ett meddelandecenter, ett kryptograficenter och sändande stationer och mottagande stationer.	Communications Centre	An organization responsible for handling and controlling communications traffic, normally comprising a message centre, a cryptographic centre, and transmitting and receiving stations.
Konfidentialitet	Egenskapen att information inte finns tillgänglig eller skyddas mot att obehöriga personer eller enheter får insyn i den.	Confidentiality	The property that information is not made available or disclosed to unauthorised individuals or entities.
Mottagande stat	En entreprenör, ett verksamhetsställe eller en annan organisation som får material från den avsändande staten	Consignee	The contractor, facility or other organization receiving material from the consignor.
Avsändande stat	En entreprenör, ett verksamhetsställe eller en annan organisation som ansvarar för organisering och avsändning av material.	Consignor	The contractor, facility or other organization responsible for organizing and dispatching material.
Kontrakt	Ett rättsligt bindande avtal om tillhandahållande av varor eller tjänster.	Contract	A legally enforceable agreement to provide goods or services.
Entreprenör	En industriell, kommersiell eller annan enhet som samtycker till att tillhandahålla varor eller tjänster	Contractor	An industrial, commercial or other entity that agrees to provide goods or services.
Kurir	En person som officiellt fått i uppdrag att personligen överlämna material.	Courier	A person officially assigned to hand-carry material.

Kurirtjänst	En tjänst som tillhandahåller personal som officiellt fått i uppdrag att personligen överlämna material.	Courier Service	A service that provides personnel officially assigned to hand-carry material.
Kryptomaterial	Innefattar kryptoalgoritmer, maskinvara för kryptering och programvarumoduler samt produkter inklusive tillämpningsdetaljer med tillhörande dokumentation och nyckelmaterial (för både symmetriska och asymmetriska kryptografiska mekanismer).	Cryptomaterial	Includes cryptographic algorithms and cryptographic hardware – and software-modules and products including implementation details and associated documentation and keying material (for both, symmetric and asymmetric cryptographic mechanisms).
Utsedd säkerhetsmyndighet (DSA)	En myndighet som ansvarar för att informera industrin om den nationella strategin i alla frågor som gäller Natos industrisäkerhetsstrategi och för att ge ledning och bistånd vid dess genomförande. I vissa länder kan en utsedd säkerhetsmyndighets verksamhet utföras av den nationella säkerhetsmyndigheten.	Designated Security Authority (DSA)	An authority responsible for communicating to industry the national policy in all matters of NATO industrial security policy and for providing direction and assistance in its implementation. In some countries, the function of a DSA may be carried out by the NSA.
Handling	All lagrad information oavsett fysisk form eller egenskaper, vilket inbegriper men inte inskränker sig till skriftliga dokument och trycksaker, hålkort och hålremsor, kartor, diagram, fotografier, målningar, ritningar, gravyrer, skisser, arbetsanteckningar och arbetsdokument, karbonkopior eller färgband, eller återgivning, oberoende av på vilket sätt eller med vilken metod de görs, samt alla slags ljud- och	Document	Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies or ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or

	röstupptagningar, magnetiska, elektroniska och optiska upptagningar och videoupptagningar, bärbar it-utrustning med fasta lagringsmedier och löstagbara lagringsmedier för datorer.		video recordings in any form, and portable IT equipment with resident computer storage media, and removable computer storage media.
Dynamisk riskhantering	Förmåga att utföra riskhantering på så sätt att risken för att använda ett kommunikations- och informationssystem kontinuerligt bedöms, att alla förändringar i det sammanhang där kommunikations- och informationssystemet fungerar återspeglas dynamiskt i koden för risken och att de säkerhetsmotåtgärder som är lämpligast i situationen i fråga genomförs rättidigt.	Dynamic Risk Management	The ability to perform risk management in a way that the risk of using a CIS is continuously assessed, any change in the context in which the CIS operates is reflected in the risk signature dynamically and the security countermeasures, most appropriate to the situation, are applied timely.
Ledsagare	Beväpnad eller obehäpnad nationell polis, militärperson eller annan statlig personal. Deras uppgift är att underlätta en säker förflyttning av materialet, men de har inget direkt ansvar i frågor som gäller skyddet av själva materialet.	Escorts	Armed or unarmed national police, military, or other government personnel. Their function is to facilitate the secure movement of the material, but they do not have direct responsibility in matters of the protection of the material itself.
Verksamhetsställe	En anläggning, ett industrikomplex, en fabrik, ett laboratorium, ett kontor, ett universitet eller en annan läroanstalt eller ett kommersiellt företag, inklusive tillhörande lager, lagringsutrymmen, förråd och komponenter som när de är kopplade	Facility	An installation, plant, factory, laboratory, office, university or other educational Institution, or commercial undertaking, including any associated warehouses, storage areas, utilities and components which, when related by function and

	till varandra genom verksamhet och plats bildar en operativ helhet.		location, form an operating entity.
Godkänd säkerhetsprövning av verksamhetsställe (FSC)	Ett administrativt beslut av en nationell säkerhetsmyndighet eller en utsedd säkerhetsmyndighet om att ett verksamhetsställe ur säkerhetsperspektiv är i stånd att erbjuda tillräcklig säkerhet för Natos säkerhets-skyddsklassificerade information på en viss säkerhetsskyddsklassificeringsnivå eller lägre och att verksamhetsställets personal som behöver åtkomst till Natos säkerhetsskyddsklassificerade information har godkänts vid en adekvat säkerhetsprövning och informerats om Natos säkerhetskrav som ska tillämpas på Natos säkerhetsskyddsklassificerade kontrakt.	Facility Security Clearance (FSC)	An administrative determination by a NSA/DSA that, from a security viewpoint, a facility can afford adequate security protection to NATO Classified Information of a specified security classification or below, and its personnel who require access to NATO Classified Information have been properly cleared and briefed on NATO security requirements necessary to perform on the NATO Classified Contracts.
Vakter	Beväpnad eller obeväpnad civil (statsanställda eller anställda deltagande entreprenörer) eller militär personal, som kan ges enbart säkerhetsvaktuppgifter eller en kombination av säkerhetsvaktuppgifter och andra uppgifter.	Guards	Civilian (government or participating contractor employees) or military personnel who may be armed or unarmed. They may be assigned for security guard duties only or may combine security guard duties with other duties.
Personligt överlämnande	Överföring av information genom att en person överlämnar informationen.	Hand Carriage	The transmission of information by an individual carrying that information on their person.
Värdstat	<u>Allmänt:</u> En stat där ett civilt eller militärt Natoorgan finns. <u>I samband med industri-säkerhet:</u>	Host Nation	<u>General:</u> The nation in which a NATO Civil or Military body is located.

	En stat som utsetts av ett officiellt organ inom Nato till att vara den statliga part som sluter kontrakt och säkerställer genomförandet av ett Nato-huvudkontrakt. Stater där underentreprenörskontrakt genomförs kallas inte värdstater.		<u>Industrial security:</u> The nation designated by an official body of NATO to act as the governmental agency to contract for the performance of a NATO prime contract. Nations in which sub-contracts are performed are not referred to as host nations.
Information	Kunskap som kan överföras i vilken form som helst.	Information	Knowledge that can be communicated in any form.
Informationssäkring	Information ska skyddas genom tillämpning av principen om informationssäkring, som avser en uppsättning åtgärder för uppnående av en viss nivå av förtroende för skyddet av kommunikations- och informationssystem och andra elektroniska system, icke-elektroniska system samt den information som lagras och behandlas i eller överförs till dessa system med avseende på konfidentialitet, riktighet, tillgänglighet, oavvislighet och autentisering.	Information Assurance	Information shall be protected by applying the principle of Information Assurance, which is described as the set of measures to achieve a given level of confidence in the protection of communication, information and other electronic systems, non-electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, nonrepudiation and authentication.
Förseelse	En säkerhetsförseelse är en avsiktlig eller oavsiktlig handling eller underlåtenhet som strider mot Natos säkerhetsstrategi och stödjande direktiv, men som inte leder till en faktisk eller eventuell läcka av Natos säkerhetskyddsklassificerade information (exempel: Na-	Infraction	A security infraction is an act or omission, deliberate or accidental, contrary to NATO Security Policy and supporting directives that does not result in the actual or possible compromise of NATO Classified Information (e.g. NATO Classified Information left unsecured inside a secure

	tos säkerhetsskyddsklassificerade information lämnas oskyddad i ett säkert verksamhetsställe där alla personer har godkänts vid en adekvat säkerhetsprövning, Natos säkerhetsskyddsklassificerade information läggs inte i dubbla emballage, och så vidare).		facility where all individuals are appropriately cleared, failure to double wrap NATO Classified Information, etc.).
Riktighet	Det att informationen (inklusive data, såsom chiffrerad text) inte har ändrats eller utplånats på ett otillåtet sätt.	Integrity	The property that information (including data, such as cipher text) has not been altered or destroyed in an unauthorised manner.
Internationella besök	Besök som av personal som omfattas av en nationell säkerhetsmyndighets eller en utsedd säkerhetsmyndighets behörighet eller som kommer från ett Natoorgan görs hos sådana verksamhetsställen eller organ som omfattas av en annan nationell säkerhetsmyndighets eller en annan utsedd säkerhetsmyndighets eller Natos behörighet, varvid besöken kräver eller kan medföra åtkomst till Natos säkerhetsskyddsklassificerade information eller varvid de oberoende av den berörda informationens säkerhetsskyddsklassificeringsnivå ska godkännas av den nationella säkerhetsmyndigheten eller den utsedda säkerhets-	International Visits	Visits made by individuals subject to one NSA/DSA or belonging to a NATO body, to facilities or bodies subject to another NSA/DSA or to NATO, which will require, or may give rise to access to NATO Classified Information or where, regardless of the level of classification involved, national legislation governing the establishment or body to be visited in support of NATO approved related activities requires that such visits shall be approved by the relevant NSA/DSA. All NATO Civil and Military bodies fall within the security jurisdiction of NATO.

	myndigheten i fråga i enlighet med den nationella lagstiftning som styr den inrättning eller det organ där ett besök som stöder av Nato godkänd anknytande verksamhet görs. Alla Natos civila och militära organ omfattas av Natos jurisdiktion i fråga om säkerhet.		
Livscykel	Informationens livscykel omfattar följande skeden: planering, insamling, skapande eller framställning av information, organisering, hämtning, användning och överföring av samt återkomst till information, lagring och skydd av information och slutligen eliminering av den genom arkivering eller utplåning.	Life-cycle	Life cycle of information encompasses the stages of planning, collection, creation or generation of information; its organization, retrieval, use, accessibility and transmission; its storage and protection; and, finally, its disposition through transfer to archives or destruction.
Maskinläsbart medium	Ett medium som kan överföra data till en given avkänningsanordning.	Machine Readable Medium	A medium that can convey data to a given sensing device.
Viktigt program/projekt	Ett sådant program eller projekt av större betydelse som normalt omfattar mer än två stater och sådana säkerhetsåtgärder som sträcker sig utöver de normala grundläggande krav som anges i Natos säkerhetsstrategi.	Major Programme/Project	A programme or project of major significance, normally involving more than two nations and security measures that extend beyond the normal basic requirements described in NATO Security Policy.
Material	Material omfattar handlingar och även varje slag av maskin, utrustning/komponenter, vapen	Material	Material includes documents and also any items of machinery, equipment/components, weap-

	eller verktyg som tillverkas eller håller på att tillverkas.		ons or tools, either manufactured or in the process of manufacture.
Militärkommittén (MC)	Den högsta militära myndigheten i Nato. Militärkommittén ansvarar för den övergripande ledningen av militära angelägenheter. Militärkommittén ansvarar operativt för att de användarkrav som förelagts av strategiska befälhavare godkänns och prioriteras.	Military Committee (MC)	The highest military authority in NATO; the MC is responsible for the overall conduct of military affairs. The MC is responsible for endorsing and prioritising from an operational point of view the users' requirements submitted by Strategic Commanders.
Medborgare	Medborgare omfattar olika staters medborgare samt permanenta invånare i Kanada. Permanenta invånare i Kanada är personer som har gått igenom ett nationellt bedömningsförfarande, som inbegriper kontroll av vistelseort och kriminalregisterkontroll samt säkerhetsprövningar, och som får ett lagenligt tillstånd att vistas permanent i Kanada.	Nationals	Nationals includes "nationals of a Kingdom", "citizens of a State", and "Permanent Residents in Canada". "Permanent Residents in Canada" are individuals who have gone through a national screening process including residency checks, criminal records and security checks, and who are going to obtain lawful permission to establish permanent residence in the nation.
Nationell säkerhetsmyndighet (NSA)	En myndighet som ansvarar för säkerheten för Natos säkerhetsskyddsklassificerade information i såväl militära som civila nationella byråer och enheter i hemlandet och utomlands.	National Security Authority (NSA)	An authority which is responsible for the security of NATO Classified Information in national agencies and elements, military or civil, at home or abroad.
Nato	Med <i>Nato</i> avses Nordatlantiska fördragsorganisationen och de organ på vilka tillämpas antingen avtalet om status för	NATO	"NATO" denotes the North Atlantic Treaty Organization and the bodies governed either by the Agreement on the

	Nordatlantiska fördragsorganisationen, nationella representanter och organisationens internationella personal, undertecknat i Ottawa den 20 september 1951, eller protokollet om status för internationella militära högkvarter som inrättats i enlighet med nordatlantiska fördraget, undertecknat i Paris den 28 augusti 1952.		status of the North Atlantic Treaty Organization, National Representatives and International Staff, signed in Ottawa on 20th September, 1951 or by the Protocol on the status of International Military Headquarters set up pursuant to the North Atlantic Treaty, signed in Paris on 28th August, 1952.
Natos säkerhets-skydds-klassificerade kontrakt	Alla kontrakt som slutits av ett civilt eller militärt Natoorgan eller en medlemsstat i Nato till stöd för ett program eller projekt som finansieras eller administreras av Nato och som kräver åtkomst till Natos säkerhets-skyddsklassificerade information eller som framställer sådan information.	NATO Classified Contract	Any contract issued by a NATO Civil or Military Body or a NATO Nation in support of a NATO funded or administered programme/project that will require access to or generate NATO Classified Information.
Natos säkerhets-skydds-klassificerade information	a) <i>information</i> avser kunskap som kan överföras i vilken form som helst, b) <i>säkerhetskyddsklassificerad information</i> avser information eller material som kräver skydd mot obehörigt röjande och som med säkerhetskyddsklassificering har angetts vara sådan, c) <i>material</i> innefattar handlingar samt maskiner, utrustning och vapen som tillverkats eller är under tillverkning, d) <i>handling</i> avser all lagrad information oavsett	NATO Classified Information	(a) Information means knowledge that can be communicated in any form; (b) Classified information means information or material determined to require protection against unauthorised disclosure which has been so designated by a security classification; (c) The word "material" includes documents and also any items of machinery or equipment or weapons either manufactured or in the process of manufacture;

	fysisk form eller egenskaper, vilket inbegriper men inte inskränker sig till skriftliga dokument och trycksaker, hålkort och håltremsor, kartor, diagram, fotografier, målningar, ritningar, gravyrer, skisser, arbetsanteckningar och arbetsdokument, karbonkopior eller färgband, eller återgivning, oberoende av på vilket sätt eller med vilken metod de görs, samt alla slags ljud- och röstupptagningar, magnetiska, elektroniska och optiska upptagningar och videoupptagningar, bärbar it-utrustning med fasta lagringsmedier och löstagbara lagringsmedier för datorer.		(d) The word “document” means any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies or ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable IT equipment with resident computer storage media, and removable computer storage media.
Natoinformation	Natoinformation omfattar all säkerhetsskyddsklassificerad och icke-säkerhetsskyddsklassificerad information som sprids i Nato, oberoende av om informationen härrör från Natos civila eller militära organ eller om den erhållits från Natos medlemsstater eller från andra källor än Nato.	NATO Information	NATO information embraces all information, classified and unclassified, circulated within NATO, whether such information originates in NATO Civil or Military bodies or is received from member nations or from non-NATO sources.
Natos produktions- och logistikorganisation	Ett underordnat organ som inrättats inom ramen för Nato för genomförande av de uppgifter som följer av nordatlantiska fördraget och som Nordatlantiska rådet ger	NATO Production and Logistics Organization (NPLO)	A subsidiary body, created within the framework of NATO for the implementation of tasks arising from that Treaty, to which North Atlantic Council grants clearly defined organizational,

	ett tydligt definierat organisatoriskt, administrativt och finansiellt oberoende. Organet ska ha en styrelse och ett verkställande organ, som består av en generaldirektör och personal.		administrative and financial independence. It shall be comprised of a board of directors; and an executive body, composed of a General Manager and staff.
Natoprogram	Ett program som godkänts av rådet och som administreras av en direktion/ett kontor som inrättats av Nato i enlighet med Natobestämmelser.	NATO Programme	A Council approved programme that is administered by a NATO management/office under NATO regulations.
Natoprojekt	Ett projekt som godkänts av rådet och som administreras av en direktion/ett kontor som inrättats av Nato i enlighet med Natobestämmelser.	NATO Project	A Council approved project that is administered by a NATO management agency/office under NATO regulations.
Direktion för Natoprojektet	Ett verkställande organ för en enskild produktions- och logistikorganisation i Nato.	NATO Project Management Agency	The executive body of a NPLO.
Behovsenlig behörighet	En princip enligt vilken en potentiell informationsmottagare behöver få åtkomst till, kunskap om eller inneha information för sin tjänsteutövning eller för att tillhandahålla officiella tjänster.	Need-to-know	The principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services.
Förhandlingar	Termen omfattar alla aspekter vid slutandet av ett kontrakt eller underentreprenörskontrakt från det inledande meddelandet om avsikt att begära anbud till det slutliga beslutet om att sluta ett kontrakt eller underentreprenörskontrakt.	Negotiations	The term encompasses all aspects of awarding a contract or subcontract from the initial "notification of intention to call for bids" to the final decision to let a contract or sub-contract.

Icke-konfidentiella tjänster	Tjänster som säkerställer uppnåendet av andra säkerhetsmål än konfidentialitet i fråga om säkerhet i kommunikations- och informationssystem, det vill säga tillgänglighet, riktighet, autentisering och oavvislighet.	Non-confidentiality services	Services for CIS Security assuring security objectives other than for Confidentiality, namely Availability, Integrity, Authentication, and Non-repudiation.
Oavvislighet	En åtgärd som ger mottagaren visshet om att informationen har sänts av en viss person eller organisation och avsändaren att informationen har mottagits av de avsedda mottagarna.	Non-repudiation	The measure of assurance to the recipient that shows that information was sent by a particular person or organization and to the sender that shows that information has been received by the intended recipients.
Öppet lagringsutrymme	Ett utrymme som skapats i enlighet med säkerhetskraven för öppen lagring av säkerhetsskyddsklassificerad information och som godkänts av chefen för det civila eller militära organet	Open Storage Area	An area, constructed in accordance with security requirements and authorised by the head of the civil or military body for open storage of Classified Information.
Den som informationen härrör från	En stat eller en internationell organisation under vars överinseende information har producerats eller introducerats i Nato.	Originator	The nation or international organization under whose authority information has been produced or introduced into NATO.
Kontroll av den som informationen härrör från	En princip enligt vilken den stat, Nato eller någon annan organisation under vars överinseende information har skapats, producerats eller introducerats i Nato fastställer de regler och krav som tillämpas på användningen av denna information och bestämmer över alla ändringar under informationens hela livscykel.	Originator Control	The principle by which the nation, NATO, or other organization, under whose authority information has been created, produced, or introduced into NATO, establishes the rules and standards which apply to the use of this information and has authority over any changes throughout information life-cycle.

Medborgarskapsland	Det land där en individ är medborgare.	Parent Nation	The Nation of which an individual is a national.
Godkänd säkerhetsprövning av person (PSC)	En godkänd säkerhetsprövning av person (PSC) är ett positivt beslut genom vilket en nationell säkerhetsmyndighet eller en utsedd säkerhetsmyndighet formellt fastställer personens lämplighet att få åtkomst till information som säkerhetsskyddsklassificerats som NATO CONFIDENTIAL eller högre med hänsyn till personens lojalitet, tillförlitlighet och pålitlighet.	Personnel Security Clearance (PSC)	A PSC is a positive determination by which a NSA/DSA formally recognizes the individual's eligibility to have access to information classified NC and above taking into account their loyalty, trustworthiness and reliability.
Huvudkontrakt	Ett ursprungligt kontrakt som slutits av direktionen/kontoret för Nato-programmet/Natoprojektet.	Prime Contract	The initial contract led by a NATO Project Management/Agency/Office for a Programme/project.
Huvudentreprenör	En sådan industriell, kommersiell eller annan enhet i en medlemsstat som har slutit ett kontrakt med en direktionskontor för ett Natoprojekt om att tillhandahålla en tjänst eller tillverka en produkt inom ramen för Natoprojektet och som för sin del kan sluta underentreprenörskontrakt med eventuella underentreprenörer, om detta godkänns.	Prime Contractor	An industrial, commercial or other entity of a member nation which has contracted with a NATO Project Management Agency/Office to perform a service, or manufacture a product, in the framework of a NATO project, and which, in turn, may subcontract with potential subcontractors as approved.
Säkerhetsskyddsklassificeringshandledning för program/projekt	Den del av säkerhetsanvisningarna för program (projekt) som identifierar de delar av ett program	Programme/Project Security Classification Guide	Part of the program (project) security instructions (PSI) which identifies the elements of the program

	<p>som är säkerhetsskyddsklassificerade och fastställer nivån på säkerhetsskyddsklassificeringen. Säkerhetsskyddsklassificeringshandledningen kan utvidgas under programmets hela livscykel och de delar som innehåller information kan ges en annan säkerhetsskyddsklassificering eller en lägre säkerhetsskyddsklassificeringsnivå.</p>		<p>that are classified, specifying the security classification levels. The security classification guide may be expanded throughout the program life cycle, and the elements of information may be re-classified or downgraded.</p>
<p>Säkerhets-anvisningar för program/projekt (PSI)</p>	<p>En sammanställning av säkerhetsbestämmelser/säkerhetsförfaranden baserad på Natos säkerhetsstrategi och stödjande direktiv, vilka tillämpas på ett specifikt projekt/program för att standardisera säkerhetsförfarandena. Säkerhetsanvisningarna för program/projekt utgör också en av bilagorna till huvudkontraktet och kan ändras under programmets hela livscykel. En tilläggs klausul om säkerhet i underentreprenörskontrakt som sluts inom programmet grundar sig på säkerhetsanvisningarna för program/projekt.</p>	<p>Programme/Project Security Instruction (PSI)</p>	<p>A compilation of security regulations/procedures, based upon NATO Security Policy and supporting directives, which are applied to a specific project/programme in order to standardise security procedures. The PSI also constitutes an Annex to the main contract, and may be revised throughout the programme lifecycle. For subcontracts let within the program, the PSI constitutes the basis for the SAL.</p>
<p>Rekommenderad postförsändelse</p>	<p>En posttjänst som gör det möjligt att spåra försändelsen från avsändaren till mottagaren och ger avsändaren ett bevis på att försändelsen levererats.</p>	<p>Registered Mail</p>	<p>A mail service that enables the possibility to track the shipment from the sender to the recipient and allows the sender a proof of the delivery.</p>

Utlämnande av information	Tillåtelse av att en mottagande enhet tar emot information på så sätt att informationen anses vara tillgänglig för hela enheten. Utlämnandet av information kan underlättas av att en person företräder enheten i fråga.	Release of information	The act of authorizing a recipient entity to receive information with the understanding that this information will be available to the entire entity. The release may be facilitated through an individual representing the entity in question.
Risk	Sannolikheten för att ett hot förverkligas på grund av en sårbarhet, varvid konfidentialitet, riktighet och/eller tillgänglighet äventyras och en skada uppstår.	Risk	The likelihood of a vulnerability being successfully exploited by a threat, leading to a compromise of confidentiality, integrity and/or availability and damage being sustained.
Riskhantering	Ett systematiskt tillvägagångssätt baserat på bedömning av hot och sårbarheter för att fastställa vilka säkerhetsmotåtgärder som krävs för att skydda informationen och de stödjande tjänsterna och resurserna. Riskhantering omfattar planering, organisering, styrning och kontroll av de resurser som säkerställer att risken hålls inom godtagbara gränser.	Risk Management	A systematic approach to determining which security countermeasures are required to protect information and supporting services and resources, based upon an assessment of the threats and vulnerabilities. Risk management involves planning, organising, directing and controlling resources to ensure that the risk remains within acceptable bounds.
Riskägare	En person eller ett organ som ansvarar för att bedöma hot, sårbarheter och effekter i fråga om vilken risk som helst i syfte att fastställa en lämplig riskaptit på grundval av faktiska förmildrande faktorer	Risk Owner	The individual or body that is charged with the responsibility of assessing the threats, vulnerabilities and impacts of any given risk with a view to establishing an appropriate risk appetite based upon the implementation of mitigating factors.

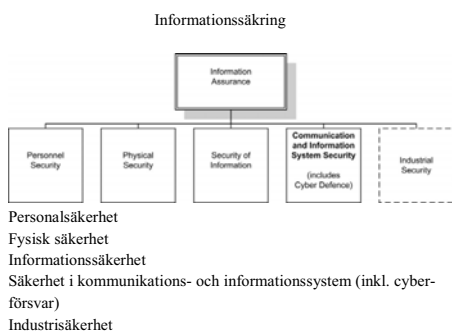
Tilläggs klausul om säkerhet (SAL)	En handling som en behörig myndighet bifogar till ett annat av Nato säkerhetsskyddsklassificerat kontrakt eller underentreprenörskontrakt än ett kontrakt som gäller viktiga program/projekt och där tillämpliga säkerhetskrav eller de delar av kontraktet som kräver skydd av informationssäkerheten specificeras.	Security Aspects Letter (SAL)	A document, issued by the appropriate authority, as part of any NATO classified contract or sub-contract, other than Major Programmes/Projects, identifying the security requirements or those elements thereof requiring security protection.
Säkerhetsgaranti	En garanti som tillhandahålls Nato antingen direkt eller genom en medlemsstat i Nato eller, när information lämnas ut, genom ett sådant civilt eller militärt organ i Nato som är säkerhetsgarant för givandet, så att en mottagare som inte hör till Nato och som får Natos säkerhetsskyddsklassificerade informationer informationen ett skydd som motsvarar det skydd som Natos säkerhetsstrategi kräver.	Security Assurance	A guarantee provided to NATO either directly or through a NATO Nation or NATO Civil or Military body sponsoring release, that a non-NATO recipient of NATO Classified Information will provide the same degree of protection to it as required by NATO Security Policy.
Säkerhetsöverträdelse	En avsiktlig eller oavsiktlig handling eller underlåtenhet som strider mot Natos säkerhetsstrategi och stödjande direktiv och som leder till ett faktiskt eller eventuellt äventyrande av Natos säkerhetsskyddsklassificerade information eller de stödjande tjänsterna och resurserna (exempel: säkerhetsskyddsklassificerad information försvinner under transporten, sä-	Security Breach	An act or omission, deliberate or accidental, contrary to NATO Security Policy and supporting directives, that results in the actual or possible compromise of NATO Classified Information or supporting services and resources (including, for example, classified information lost while being transported; classified information left in an unse-

	kerhetsskyddsklassificerad information lämnas i ett oskyddat utrymme dit personer som inte har godkänts vid säkerhetsprövning har obeleddat tillträde, en handling som omfattas av ansvarsskyldighet för säkerheten kan inte hittas, otillåten ändring av säkerhetsskyddsklassificerad information, utplåning av säkerhetsskyddsklassificerad information på obehörigt sätt eller överbelastning av tjänsterna i kommunikations- och informationssystem).		cured area where un-cleared individuals have unescorted access; an accountable document cannot be found; classified information has been subjected to unauthorised modification; destroyed in an unauthorised manner or, for CIS, there is a denial of service).
Minneslista för säkerhetsskyddsklassificering	Den del av en tilläggs-klausul om säkerhet som anger vilka delar av kontraktet som är säkerhetsskyddsklassificerade och fastställer nivån på säkerhetsskyddsklassificeringen. Säkerhetsskyddsklassificeringen för delar i kontrakt som slutits inom ett program/projekt grundar sig på säkerhetsanvisningarna för program/projekt.	Security Classification Check List	Part of a security aspect letter (SAL) which describes the elements of a contract that are classified, specifying the security classification levels. In case of contracts let within a program/project, such elements of information derive from the programme (project) security instructions issued for that programme.
Säkerhetsnycklar	Säkerhetsnycklar är nycklar som används i lås på säkerhetsskåp för förvaring av säkerhetsskyddsklassificerat material, dörrar till säkra rum eller utrymmen, dörrar till säkra rum eller utrymmen som har varit föremål för tekniska säkerhetsinspektioner och	Security Keys	Security keys are those which operate the locks fitted to: secure cabinets provided for the storage of classified material; doors of secure rooms or areas; doors of secure rooms or areas which have been subject to technical security inspections; and secure cabinets

	säkerhetsskåp som används för spridning av säkerhetsskyddsklassificerade handlingar.		used for the circulation of classified documents.
Säkerhetsincident	En händelse eller någon annan tilldragelse som kan ha en negativ inverkan på säkerheten för Natos säkerhetsskyddsklassificerade information och som kräver ytterligare utredningsåtgärder för exakt avgörande av om händelsen eller tilldragelsen utgör en säkerhetsöverträdelse eller säkerhetsförseelse.	Security Incident	An event or other occurrence that may have an adverse effect upon the security of NATO Classified Information which requires further investigative actions in order to accurately determine whether or not it constitutes a Security Breach or Infraction.
Information av särskild kategori	Information på vilken ytterligare hanterings-/skyddsförfaranden tillämpas, till exempel ATOMAL, gemensam operativ plan (SIOP), BOHEMIA eller CRYPTO.	Special Category Information	Information such as ATOMAL, Single Integrated Operational Plan (SIOP), BOHEMIA or CRYPTO to which additional handling/protection procedures are applied.
Garant	Ett Natoland eller ett civilt eller militärt Natoorgan som fungerar som garant när det gäller att ge behövliga garantier för att en enhet som inte hör till Nato och som mottar säkerhetsskyddsklassificerad information från Nato ger denna information behövligt skydd i enlighet med de grundläggande principer och krav som anges i Natos säkerhetsstrategi och stödjande direktiv.	Sponsor	A NATO Nation or a NATO Civil or Military body acting as a guarantor in providing the necessary assurance that a NNE in receipt of NATO Classified Information will afford that information the necessary protection in line with the basic principles and requirements as set out in NATO Security Policy and supporting directives.
Underentreprenörs-kontrakt	Ett kontrakt som slutits av en huvudentreprenör med en annan entreprenör (underentreprenör)	Sub-contract	A contract entered into by a prime contractor with another contractor (i.e., the sub-contractor)

	om att tillhandahålla varor eller tjänster.		for the furnishing of goods or services.
Underentreprenör	En entreprenör som en huvudentreprenör sluter ett underkontrakt med.	Sub-contractor	A contractor to whom a prime contractor lets a sub-contract.
Hot	Potentialen för läckor, förlust eller stöld när det gäller Natos säkerhets- skyddsklassificerade information eller de stödjande tjänsterna och resurserna. Ett hot kan definieras genom dess källa, motiv eller resultat och det kan vara avsiktligt eller oavsiktligt, våldsamt eller dolt, externt eller internt.	Threat	The potential for compromise, loss or theft of NATO Classified Information or supporting services and resources. A threat may be defined by its source, motivation or result, it may be deliberate or accidental, violent or surreptitious, external or internal.
Sårbarhet	En svaghet, en egenskap eller en avsaknad av tillsyn som möjliggör eller underlättar att ett hot mot Natos säkerhetsskyddsklassificerade information eller de stödjande tjänsterna och resurserna förverkligas.	Vulnerability	A weakness, an attribute, or lack of control that would allow or facilitate a threat actuation against NATO Classified Information or supporting services and resources.

*Bilaga F, Figur 1



Figur 1 – Förhållandet mellan informationssäkring och säkerhet i kommunikations- och informationssystem (CIS Security)

*Enclosure F, Picture 1



Figure 1 - Relationship between Information Assurance and CIS Security