NORTH ATLANTIC COUNCIL
CONSEIL DE L'ATLANTIQUE NORD

NATO NEUTAJOVANÉ

17. júna 2002

DOKUMENT C-M(2002)49

VRÁTANE COR 1 až 12

BEZPEČNOSŤ V RÁMCI ORGANIZÁCIE SEVEROATLANTICKEJ ZMLUVY (NATO)

Oznámenie generálneho tajomníka

Referencia: C-M(2002)23 a dokument o akcii (akčný dokument)

1. Tento dokument je výsledkom dôkladného preskúmania zo strany Bezpečnostného výboru NATO (NSC) a bol schválený Radou v tichej schvaľovacej procedúre dňa 26. marca 2002 (odkaz).

2. Tento dokument spolu s dokumentom C-M(2002)50, „Ochranné opatrenia pre civilné a vojenské orgány NATO, nasadené sily NATO a zariadenia (aktíva) proti teroristickým hrozbám“, nahrádza dokument C-M(55)15(Final). S výnimkou prílohy A „Bezpečnostná dohoda zmluvných strán Severoatlantickej zmluvy“, ktorá je naďalej platná pre tie krajiny, ktoré ešte neratifikovali „Dohodu medzi zmluvnými stranami Severoatlantickej zmluvy o bezpečnosti informácií“, musia byť všetky predchádzajúce verzie CM (55)15(Final) teraz zničené.

3. Nasledujúce smernice podporujú tento dokument:

Smernica AC/35-D/2000 o personálnej bezpečnosti
Smernica AC/35-D/2001 o fyzickej bezpečnosti
Smernica AC/35-D/2002 o administratívnej bezpečnosti
Smernica AC/35-D/2003 o priemyselnej bezpečnosti
Základná smernica AC/ 35-D/2004 o INFOSEC
Smernica AC/35-D/2005 o manažmente INFOSEC pre CIS

Prvé štyri smernice (AC/35-D/2000-2003) boli schválené Radou (vyššie uvádzané odkazy) a zvyšné dve (AC/35-D/2004 a D/2005) Bezpečnostným výborom NATO (NSC) a výborom NATO C3Board.

4. Na zjednodušenie odkazovania bude v blízkej budúcnosti distribuovaný prehľad obsahujúci dva dokumenty bezpečnostnej politiky (CM (2002)49 a CM (2002)50) a vyššie uvedené podporné smernice pre všetkých súčasných držiteľov C-M(55)15(Final).

(Podpísaný) George Robertson

Originál: Angličtina

NATO NEUTAJOVANÉ

ZÁZNAM DOPLNENÍ/ O NOVELIZÁCIÁCH

Preškrtnite zodpovedajúce číslo pri vložení každého doplnenia/každej novelizácii

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

C-M (2002)49

OBSAH

Oznámenie generálneho tajomníka

Záznam doplnení/novelizácií

Obsah

Príloha „A“ - Bezpečnostná dohoda

Príloha „B“ - Základné zásady bezpečnosti

Príloha „C“ - Personálna bezpečnosť

Príloha „D“ - Fyzická bezpečnosť

Príloha „E“ - Administratívna bezpečnosť

Príloha „F“ - Bezpečnosť CIS (cor. 9; cor. 11)

Príloha „G“ – Utajovaný projekt a priemyselná bezpečnosť (cor. 12)
Slovník pojmov

PRÍLOHA „A“

DOHODA MEDZI ZMLUVNÝMI STRANAMI SEVEROATLANTICKEJ ZMLUVY O BEZPEČNOSTI INFORMÁCIÍ

Zmluvné strany Severoatlantickej zmluvy podpísanej vo Washingtone 4. apríla 1949.

Opätovne potvrdzujúc, že účinné politické konzultácie, spolupráca a obranné plánovanie na dosiahnutie cieľov zmluvy so sebou prinášajú výmenu utajovaných skutočností medzi stranami zmluvy.

Uznávajúc, že ustanovenia medzi vládami strán Severoatlantickej zmluvy ohľadom vzájomnej ochrany a zabezpečenia utajovaných skutočností, ku výmene ktorých môže dochádzať, sú nevyhnutné.

Uvedomujúc si potrebu všeobecného systému pre bezpečnostné normy a postupy.

Konajúc vo svojom vlastnom mene a v mene Organizácie Severoatlantickej zmluvy, dohodli sa nasledovne:

ČLÁNOK 1

Strany sa zaväzujú:

(i) chrániť a zabezpečovať:

(a) utajované skutočností (pozri DODATOK 1) takto označené, ktorých pôvodcom je NATO (pozri DODATOK 2), alebo ktoré NATO postúpila členská krajina,

(b) utajované skutočností takto označené, postúpené členskými krajinami inej členskej krajine, s cieľom podpory programu, projektu alebo kontraktu NATO,

(ii) zachovávať stupeň utajenia skutočností definovaných v bode (i) a vynaložiť každé úsilie na ich adekvátne zabezpečenie,

(iii) nepoužívať utajované skutočnosti definované v bode (i) na iné účely než tie, ktoré stanovuje Severoatlantická zmluva a k nej prináležiace rozhodnutia a rezolúcie,

(iv) neposkytovať takéto utajované skutočnosti, definované v bode (i), stranám, ktoré nie sú signatármi Severoatlantickej zmluvy bez súhlasu ich pôvodcu.

ČLÁNOK 2

V súlade s článkom 1 tejto dohody sa strany zaväzujú zabezpečiť vytvorenie národného bezpečnostného úradu pre činnosti NATO, ktoré zavedú ochranné bezpečnostné opatrenia. Strany zriadia a zavedú do praxe bezpečnostné normy, ktoré zabezpečia spoločný stupeň ochrany utajovaných skutočností.

ČLÁNOK 3

(1) Strany sa zaväzujú zabezpečiť, aby všetky osoby ich štátnej príslušnosti, ktorých výkon úradných povinností vyžaduje alebo umožňuje prístup k informáciám stupňa utajenia CONFIDENTIAL a vyššie, boli primerane preverené ešte predtým, než sa ujmú svojich povinností.

(2) Postupy bezpečnostnej previerky sa vytvoria tak, aby na ich základe bolo možné stanoviť, či osoba, berúc do úvahy jeho/jej lojalitu a dôveryhodnosť, môže mať prístup k utajovaným skutočnostiam bez toho, aby predstavovala neprijateľné riziko pre bezpečnosť.

(3) Na základe požiadavky poskytne ktorákoľvek zo strán súčinnosť ostatným stranám pri výkone ich vlastných bezpečnostných previerok.

ČLÁNOK 4

Generálny tajomník zabezpečí, aby sa v NATO aplikovali príslušné ustanovenia tejto dohody (pozri DODATOK 3)

ČLÁNOK 5

Táto dohoda žiadnym spôsobom stranám nebráni uzatvárať ďalšie dohody v oblasti výmeny utajovaných skutočností, ktorých sú pôvodcami, ak tým neovplyvnia rozsah tejto dohody.

ČLÁNOK 6

(a) Táto dohoda je otvorená na podpis zmluvným stranám Severoatlantickej zmluvy a podlieha ratifikácii, prijatiu alebo schváleniu. Ratifikačné listiny, listiny o prijatí alebo schválení sa uložia u vlády

Spojených štátov amerických.

(b) Táto dohoda nadobudne platnosť 30 dní odo dňa uloženia ratifikačných listín, listín o prijatí alebo schválení dvoma signatárskymi krajinami. Pre každú ďalšiu signatársku krajinu dohoda nadobudne platnosť 30 dní odo dňa uloženia jej ratifikačnej listiny, listiny o prijatí alebo schválení.

(c) Pre strany, pre ktoré táto dohoda nadobudla platnosť, nahradí „Bezpečnostnú dohodu strán Organizácie Severoatlantickej zmluvy“ schválenú Severoatlantickou radou v Prílohe A (odsek 1)

k dodatku prílohy D.C. 2/7 z 19. apríla 1952 a následne začlenenú do prílohy A (odsek 1) do CM(55)15(final), schválenú Severoatlantickou radou dňa 2. marca

ČLÁNOK 7

Táto dohoda zostane otvorená na prístup každej novej strany Severoatlantickej zmluvy v súlade s jej vlastnými ústavnými postupmi. Jej listina o pristúpení bude uložená u vlády Spojených štátov amerických. Nadobudne platnosť pre každú pristupujúcu krajinu 30 dní odo dňa uloženia jeho listiny o prístupe.

ČLÁNOK 8

Vláda Spojených štátov amerických bude informovať vlády ostatných strán o uložení každej ratifikačnej listiny, listiny o prijatí, schválení alebo prístupe.

ČLÁNOK 9

Túto dohodu môže vypovedať ktorákoľvek strana písomným oznámením o výpovedi podaným depozitárovi, ktorý bude informovať všetky ostatné strany o takomto oznámení. Takáto výpoveď nadobudne účinnosť jeden rok po prijatí oznámenia depozitárom, neovplyvní však povinnosti už zmluvne upravené a práva alebo výsady predtým nadobudnuté stranami na základe ustanovení tejto dohody.

Na dôkaz toho, dolu podpísaní, riadne na to splnomocnení svojimi príslušnými vládami, podpísali túto dohodu.

V Bruseli dňa ..... xxxx v jednom vyhotovení v anglickom a francúzskom jazyku, pričom obe znenia majú rovnakú platnosť, ktoré sa uloží v archívoch vlády Spojených štátov amerických a ktorého overené kópie budú odovzdané touto vládou každému zo zvyšných signatárov.

PRÍLOHA „A“
C-M(2002)0049

DODATOK 1

Tento dodatok tvorí neoddeliteľnú súčasť dohody.

Utajované skutočnosti NATO sú definované nasledovne:

(a) informácia je definovaná ako poznatok, ktorý môže byť sprostredkovaný akoukoľvek formou,

(b) utajovaná skutočnosť je definovaná ako informácia alebo vec, ktorá je predmetom ochrany pred neoprávneným zverejnením, a bola takto označená príslušným stupňom utajenia,

(c) slovo „materiál“ zahŕňa dokumenty a taktiež akúkoľvek súčasť mechanizmu, zariadenia, alebo zbraní či už vyrobených alebo v procese výroby,

(d) slovo „dokument“ znamená akúkoľvek zaznamenanú informáciu, bez ohľadu na jej fyzickú formu alebo charakter, vrátane, ale nie len, písaných alebo tlačených údajov, kariet a pások na záznam údajov, máp, tabuliek, fotografií, malieb, kresieb, rytín, nákresov, pracovných poznámok a papierov, kópií z kopírovacích papierov a atramentových pások alebo reprodukcií vyrobených akýmikoľvek prostriedkami alebo postupmi, hlasových, zvukových, magnetických, elektronických, optických alebo obrazových záznamov v akejkoľvek forme, prenosných zariadení automatického spracovania dát s príslušným počítačovým pamäťovým médiom a prenosných počítačových pamäťových médií.

DODATOK 2

Tento dodatok tvorí neoddeliteľnú súčasť dohody.

Na účely tejto dohody pojem „NATO“ označuje Organizáciu Severoatlantickej zmluvy a orgány riadiace sa buď Dohodou o štatúte Organizácie Severoatlantickej zmluvy, národných predstaviteľov a Medzinárodného štábu, podpísanou v Ottawe dňa 20. septembra 1951, alebo Protokolom o štatúte Hlavného medzinárodného vojenského veliteľstva, zriadeného na základe Severoatlantickej zmluvy, podpísaného v Paríži dňa 28. augusta 1952.

DODATOK 3

Tento dodatok tvorí neoddeliteľnú súčasť dohody.

Konzultácie sa uskutočňujú s vojenskými veliteľmi za účelom rešpektovania ich výsad.

PRÍLOHA „B“
C-M(2002)0049

PRÍLOHA „B“

ZÁKLADNÉ PRINCÍPY A MINIMÁLNE ŠTANDARDY BEZPEČNOSTI

1. ÚVOD

1.1. Tento C-M dokument stanovuje základné zásady a minimálne bezpečnostné štandardy, ktoré majú uplatňovať členské krajiny NATO a civilné a vojenské orgány NATO, aby bola zabezpečená spoločná úroveň ochrany utajovaných skutočností, ktoré si strany vymieňajú. Bezpečnostné postupy NATO fungujú najlepšie/najefektívnejšie, ak sú založené a podporované národným bezpečnostným systémom, ktorý má charakteristiky uvedené v tejto prílohe. Táto príloha sa zaoberá aj bezpečnostnými povinnosťami v rámci NATO.

2. ZÁMERY A CIELE

2.1. Členské krajiny NATO a civilné a vojenské orgány NATO zabezpečia, aby sa základné princípy a minimálne bezpečnostné normy stanovené v tomto C-M dokumente používali na ochranu utajovaných skutočností pred stratou ich dôvernosti, integrity a dostupnosti.

2.2. Členské krajiny NATO a civilné a vojenské orgány NATO vytvoria bezpečnostné programy, ktoré spĺňajú tieto základné princípy a minimálne štandardy, aby zabezpečili spoločný stupeň ochrany utajovaných skutočností.

3. POUŽITEĽNOSŤ

3.1. Tieto základné zásady a minimálne štandardy sa uplatňujú na:

(a) utajované skutočnosti, ktorých pôvodcom je NATO, ktoré vznikli v členskej krajine a ktoré boli predložené NATO alebo predložené členskou krajinou inej členskej krajine na podporu programu, projektu alebo zmluvy NATO,

(b) utajované skutočnosti, ktoré NATO získalo zo zdrojov mimo NATO, a

(c) utajované skutočnosti zverené osobám a organizáciám mimo orgánov štátnej správy (alebo civilného alebo vojenského orgánu NATO), napr. konzultantom, priemyslu, univerzitám, ktoré ich chránia podľa rovnakých štandardov uplatňovaných vládou alebo civilným alebo vojenským orgánom NATO.

Máj 2013
Doplnok č. 10

3.2. Prístup k utajovaným skutočnostiam ATOMAL a ich ochrana podlieha Dohode medzi stranami Severoatlantickej zmluvy o spolupráci v oblasti utajovaných skutočností ATOMAL - C-M(64)39. Administratívne opatrenia na vykonávanie Dohody medzi zmluvnými stranami Severoatlantickej zmluvy o spolupráci týkajúcej sa utajovaných skutočností ATOMAL - aktuálna verzia CM (68) 41 - sa budú uplatňovať pri kontrole prístupu k týmto informáciám, ich manipulácii a ochrane.

3.3. Prístup k utajovaným skutočnostiam US-SIOP a ich ochrana podliehajú ustanoveniam dokumentu C-M(71)27(Revised), „Osobitné postupy pre manipulovanie s informáciami Jednotného integrovaného operačného plánu USA (US-SIOP) v rámci NATO“.

3.4. Citlivosť šifrových informácií, opatrení a produktov vyžaduje uplatnenie prísnych bezpečnostných opatrení, ktoré často presahujú rámec stanovený v tomto dokumente. Prístup ku šifrovým informáciám, opatreniam a produktom, ktoré sú schválené na národnej úrovni alebo NAMILCOM, musí byť preto v súlade s prílohou „F“, podpornými smernicami a postupmi stanovenými príslušným orgánom.

3.5. Citlivá povaha informácií signálneho spravodajstva (SIGINT), operácií, zdrojov a metód Politiky signálneho spravodajstva (SIGINT) vyžaduje použitie prísnych bezpečnostných predpisov a postupov, ktoré často presahujú rámec stanovený v tomto dokumente. Preto prístup k informáciám, operáciám, zdrojom a metódam SIGINT a ich ochrana podliehajú vnútroštátnym predpisom a ustanoveniam vymedzených v MC 101 (Politika signálového spravodajstva NATO/NATO Signals Intelligence Policy) a v jeho príručke Spoločnej spojeneckej publikácie (AJP).

4. PRÁVOMOC

4.1. Severoatlantická rada (NAC) schválila tento dokument, ktorým sa implementuje Dohoda medzi stranami Severoatlantickej zmluvy o bezpečnosti informácií (uvedená v Prílohe A), čím sa ustanovuje Bezpečnostná politika NATO.

5. ZÁKLADNÉ PRINCÍPY

5.1. Uplatňujú sa tieto základné princípy:

(a) Členské štáty NATO a civilné a vojenské orgány NATO zabezpečia, aby sa dohodnuté minimálne štandardy stanovené v tomto dokumente použili na zabezpečenie spoločného stupňa ochrany utajovaných skutočností, ktoré si strany vymieňajú,

(b) utajované skutočnosti sa sprístupnia výlučne na základe princípu „need-to-know“ osobám, ktoré boli poučené o príslušných bezpečnostných postupoch; navyše prístup k informáciám so stupňom utajenia CONFIDENTIAL a vyšším majú len osoby s bezpečnostnou previerkou,

(c) manažment bezpečnostného rizika je povinný v rámci civilných a vojenských orgánov NATO. Jeho uplatňovanie v rámci krajín NATO je dobrovoľné,

(d) utajované skutočnosti musia byť chránené vyváženým súborom bezpečnostných opatrení vrátane personálnej bezpečnosti, fyzickej bezpečnosti, administratívnej bezpečnosti, bezpečnosti komunikačných a informačných systémov (bezpečnosť CIS), ktorá sa vzťahuje na všetky osoby, ktoré majú prístup k utajovaným skutočnostiam, všetkým médiám prenášajúcim utajované skutočnosti a do všetkých priestorov obsahujúcich takéto utajované skutočnosti,

(e) koordinácia riadenia vnútorných hrozieb s príslušnými národnými autoritami a civilnými a vojenskými orgánmi NATO,

(f) členské krajiny NATO a civilné a vojenské orgány NATO vypracujú programy bezpečnostného povedomia a školenia vo všetkých oblastiach bezpečnosti uvedených v odseku 5.1 písm. d) vyššie,

(g) všetky podozrenia z porušenia bezpečnosti sa okamžite oznámia príslušnému bezpečnostnému úradu. Hlásenia vyhodnotia príslušní úradníci s cieľom posúdiť vzniknuté škody voči NATO s prijatím vhodných opatrení. Príloha E uvádza podrobnosti,

(h) pôvodcovia uvoľňujú utajované skutočnosti NATO a krajinám NATO na podporu programu, projektu alebo zmluvy NATO s tým, že sa s nimi bude manipulovať a budú chránené v súlade s Politikou spravovania informácií NATO (NIMP) a Bezpečnostnou politikou NATO,

(i) utajované skutočnosti podliehajú kontrole zo strany pôvodcu,

(j) uvoľňovanie utajovaných skutočností musí byť v súlade s požiadavkami prílohy E k tomuto C-M dokumentu a podpornými smernicami, a

(k) so súhlasom pôvodcu a v súlade s prílohou E k tomuto C-M dokumentu sa utajované skutočnosti NATO uvoľnia iba tým nečlenským krajinám a organizáciám, ktoré buď podpísali bezpečnostnú dohodu s NATO, alebo ktoré poskytli bezpečnostnú záruku NATO, a to buď priamo, alebo prostredníctvom krajiny NATO alebo civilného alebo vojenského orgánu NATO zabezpečujúceho uvoľnenie informácií. Vo všetkých prípadoch pre akékoľvek uvoľnenie utajovaných skutočností NATO sa vyžaduje rovnaký stupeň ochrany ako v tomto C-M dokumente.

5.2. Základy stabilnej národnej bezpečnosti sú:

(a) bezpečnostná organizácia zodpovedná za:

i) zhromažďovanie a zaznamenávanie spravodajských informácií týkajúcich sa špionáže, terorizmu, sabotáže a podvratných hrozieb, a

(ii) centralizáciu takýchto informácií tak, aby sa mohli uplatňovať na akúkoľvek situáciu týkajúcu sa zamestnávania osôb vo vládnych rezortoch a agentúrach, a dodávateľmi, a

(iii) poskytovanie informácií a poradenstva vládam o povahe hrozieb pre bezpečnosť a prostriedkoch ochrany proti nim, a

(b) pravidelná spolupráca medzi vládnymi rezortmi a agentúrami s cieľom:

i) identifikovať utajované skutočnosti, ktoré je potrebné chrániť, a

ii) stanoviť a uplatňovať spoločné stupne ochrany, v súlade s týmto C-M dokumentom.

5.3. **Personálna bezpečnosť**

5.3.1. Postupy pre personálnu bezpečnosť musia byť navrhnuté tak, aby určili, či môže osoba, pri zohľadnení jej lojality, dôveryhodnosti a spoľahlivosti, získať oprávnenie na prístup k utajovaným skutočnostiam bez toho, aby to predstavovalo neprijateľné riziko pre bezpečnosť. Všetky osoby,

civilné a vojenské, ktoré vyžadujú prístup k informáciám so stupňom utajenia CONFIDENTIAL alebo vyšším, alebo ktorých povinnosti alebo funkcie môžu poskytnúť prístup k takýmto informáciám, musia byť príslušným spôsobom preverené a poučené predtým, ako im bude takýto prístup udelený. Jednotlivci majú prístup iba k tým utajovaným skutočnostiam NATO, na ktoré je možné uplatniť princíp „need-to-know“.

5.3.2. Bezpečnostná previerka sa nevyžaduje pre prístup k informáciám so stupňom utajenia RESTRICTED, pričom osoby budú poučené o svojich povinnostiach pri ochrane utajovaných skutočností so stupňom utajenia RESTRICTED.

5.3.3. Personálna bezpečnosť je ďalej riešená v prílohe "C" tohto C-M a v podpornej smernici o personálnej bezpečnosti.

5.4. **Fyzická bezpečnosť**

5.4.1. Fyzická bezpečnosť predstavuje použitie fyzických ochranných opatrení na miesta, budovy alebo zariadenia, ktoré obsahujú informácie vyžadujúce ochranu pred stratou alebo poškodením. Programy fyzickej bezpečnosti pozostávajúce z aktívnych a pasívnych bezpečnostných opatrení sa stanovia tak, aby poskytovali úrovne fyzickej bezpečnosti konzistentné s hrozbou, bezpečnostnou klasifikáciou a množstvom informácií, ktoré sa majú chrániť.

5.4.2. Fyzická bezpečnosť je ďalej riešená v prílohe "D" tohto C-M dokumente a v podpornej smernici o fyzickej bezpečnosti.

5.5. **Administratívna bezpečnosť**

5.5.1. Administratívna bezpečnosť je aplikovanie všeobecných ochranných opatrení a postupov na prevenciu, detekciu a obnovu pri strate alebo poškodení informácií. Utajované skutočnosti sú počas svojho životného cyklu chránené na úrovni zodpovedajúcej ich úrovni utajenia. Musia byť spracované tak, aby boli riadne utajené, jasne označené a v režime utajenia len na nevyhnutne dlhé obdobie.

5.5.2. Bezpečnostné stupne utajenia sa budú uplatňovať na informácie, ktoré naznačujú možné poškodenie bezpečnosti NATO a/alebo jej členských krajín, ak sú informácie predmetom neoprávneného prístupu. Bezpečnostné stupne utajenia NATO sa uplatňujú v súlade s prílohou E k tomuto C-M dokumentu. Je výhradným právom pôvodcu informácií určiť alebo zmeniť stupeň bezpečnostného utajenia.

5.5.3. Stupne utajenia NATO a ich význam:

(a) COSMIC TOP SECRET (CTS):
neoprávnené zverejnenie by malo za následok mimoriadne vážne poškodenie NATO,

(b) NATO SECRET (NS):
neoprávnené zverejnenie by malo za následok vážne poškodenie NATO,

(c) NATO CONFIDENTIAL (NC):
neoprávnené zverejnenie by poškodilo NATO, a

(d) NATO RESTRICTED (NR):
neoprávnené zverejnenie by poškodilo záujmy alebo účinnosť NATO.

5.5.4. Pri utajovaní informácií pôvodca zohľadní škodu, ak je informácia predmetom neoprávneného zverejnenia, a ak je to možné, uvedie, či je možné znížiť stupeň utajenia alebo odtajniť v určitý deň alebo pri určitej udalosti.

5.5.5. Informácie NATO UNCLASSIFIED - zásady a postupy pre správu a ochranu neutajovaných informácií označených NATO UNCLASSIFIED sú obsiahnuté v Politike riadenia informácií NATO (NIMP).

5.5.6. Bezpečnosť informácií je ďalej riešená v prílohe E tohto C-M dokumentu a v podpornej smernici o bezpečnosti informácií/administratívnej bezpečnosti.

5.5.7. Plánovanie, príprava, vykonávanie a podpora súvisiace s operáciami, výcvikom, cvičeniami, transformáciou a spoluprácou NATO (OTETC) si môžu vyžadovať osobitné dodatočné bezpečnostné aspekty, ktoré treba riešiť; podporný dokument o zdieľaní informácií a spravodajských informácií so subjektmi, ktoré nie sú členmi organizácie NATO (NNEs) obsahuje bezpečnostné ustanovenia a usmernenia, uplatniteľné za týchto okolností.

5.6. **Bezpečnosť CIS**

5.6.1. Bezpečnosť CIS je uplatňovanie bezpečnostných opatrení na ochranu komunikačných, informačných a iných elektronických systémov a informácií, ktoré sú v týchto systémoch uložené, spracovávané alebo prenášané s ohľadom na dôvernosť, integritu, dostupnosť, autentifikáciu a nespochybniteľnosť.

5.6.2. Za účelom dosiahnutia bezpečnostných cieľov týkajúcich sa dôvernosti, integrity, dostupnosti, autentifikácie a nespochybniteľnosti sa zavedie vyvážený súbor bezpečnostných opatrení (fyzické, personálne, informačné, CIS), aby sa vytvorilo bezpečné prostredie, v ktorom sa môže prevádzkovať komunikačný, informačný alebo iný elektronický systém.

5.6.3. Bezpečnosťou CIS sa ďalej zaoberá príloha F tohto C-M dokumentu a podporné riadiace, technické a realizačné smernice o bezpečnosti CIS.

5.7. **Priemyselná bezpečnosť**

5.7.1. Priemyselná bezpečnosť je aplikovanie všeobecných ochranných opatrení a postupov na prevenciu, detekciu a obnovu pri strate alebo poškodení utajovaných skutočností, s ktorými sa v oblasti priemyslu manipuluje prostredníctvom priemyselných zmlúv. Utajované skutočnosti NATO postupované priemyslu **,** ktoré vznikli ako výsledok zmluvnej spolupráce s priemyslom a utajované zmluvy s priemyslom, sú chránené v súlade s Bezpečnostnou politikou NATO a podpornými smernicami.

5.7.2. Predtým, ako podnikateľský subjekt alebo jeho zamestnanci, manažéri alebo vlastníci môžu získať prístup k utajovaným skutočnostiam alebo môžu byť vyzvaní, aby predložili ponuky, rokovali alebo realizovali utajovaný kontrakt alebo prácu na utajovanej štúdii (výskume) zahŕňajúcej prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIAL alebo vyšším, podnikateľskému subjektu musí byť vydané potvrdenie o priemyselnej bezpečnosti od národného bezpečnostného úradu (NSA) (alebo, ak je to vhodné, určeným bezpečnostným úradom (DSA)) krajiny svojho pôvodu, t. j. štátu, v ktorom je subjekt umiestnený a zapísaný do obchodného registra.

5.8.1. Podnikateľke subjekty sú povinné chrániť utajované skutočnosti v súlade so základnými zásadami a minimálnymi štandardmi obsiahnutými v tomto C-M dokumente. Národné bezpečnostné úrady musia zabezpečiť, aby mali prostriedky na to, aby priemyselné bezpečnostné požiadavky boli pre priemysel záväzné a aby mali právo kontrolovať a schvaľovať opatrenia prijaté na ochranu utajovaných skutočností v oblasti priemyslu.

5.8.2. Priemyselnou bezpečnosťou sa ďalej zaoberá príloha G tohto C-M dokumentu a podporná smernica o priemyselnej bezpečnosti.

6. OCHRANA INFORMÁCIÍ V KĽÚČOVÝCH BODOCH

6.1. Zverejnenie informácií o civilných zariadeniach (obranné zásobovanie, zásobovanie energiou atď.) vojenského významu v čase ohrozenia alebo vojny môže napomáhať bombardovaniu, sabotáži alebo teroristickému útoku tým, že umožní potenciálnym nepriateľom zostaviť zoznam kľúčových bodov a identifikovať významné miesta pre sabotáž alebo terorizmus v rámci jednotlivých kľúčových bodov. Politika musí byť navrhnutá tak, aby zabránila zostaveniu zoznamu kľúčových bodov potenciálnymi nepriateľmi, aby sa umožnilo uplatnenie bezpečnostných výnimiek pri uverejňovaní príslušných údajov a zabezpečila sa informovanosť o rizikách medzi majiteľmi a prevádzkovateľmi týchto zariadení.

7. BEZPEČNOSTNÉ ZÁVÄZKY

7.1. **Národný bezpečnostný úrad (NSA)**

7.1.1. Každý členský štát zriadi národný bezpečnostný úrad (NSA) zodpovedný za bezpečnosť utajovaných skutočností NATO.

7.1.2. NSA je zodpovedný za:

(a) zachovávanie bezpečnosti utajovaných skutočností NATO v štátnych orgánoch a ich útvaroch, vojenských alebo civilných, doma alebo v zahraničí,

(b) zabezpečenie pravidelných a náležitých kontrol bezpečnostných opatrení na ochranu utajovaných skutočností NATO vo všetkých štátnych orgánoch na všetkých úrovniach,) a to tak vojenských, ako aj civilných, s cieľom určiť, či sú tieto opatrenia primerané a v súlade so platnými bezpečnostnými predpismi NATO. V prípade organizácií, ktoré sú držiteľmi utajovaných skutočností CTS alebo ATOMAL, sa bezpečnostné inšpekcie vykonávajú najmenej raz za 24 mesiacov, pokiaľ ich počas tejto lehoty nevykoná Bezpečnostný úrad NATO (NOS),

(c) zabezpečenie, že bezpečnostné určenie spôsobilosti sa vykonáva u všetkých štátnych príslušníkov, od ktorých sa vyžaduje prístup k utajovaným skutočnostiam stupňa NC a vyššie v súlade s Bezpečnostnou politikou NATO;

(d) zabezpečenie, aby boli vypracované také národné núdzové bezpečnostné plány, ktoré sú potrebné na zabránenie tomu, aby sa utajené informácie NATO dostali do rúk neoprávnených alebo nepriateľských rúk, a

(e) schvaľovanie zariadenia (alebo zrušenie) národných kozmických centrálnych registrov. Zriadenie (alebo zrušenie) kozmických centrálnych registrov sa oznámi BÚN.

7.2. **Určený bezpečnostný orgán (DSA)**

7.2.1. Každá členská krajina môže určiť jeden alebo viaceré DSA podliehajúce NSA. V tomto prípade je DSA krajiny NATO zodpovedný za informovanie priemyslu o národnej politike vo všetkých záležitostiach politiky priemyselnej bezpečnosti NATO a za poskytnutie usmernenia a pomoci pri jej implementácii. V niektorých krajinách môže funkciu DSA vykonávať NSA.

7.3. **Bezpečnostný výbor (SC)**

7.3.1. SC je zriadený Severoatlantickou radou (NAC) a je zložený zo zástupcov národných bezpečnostných úradov (NSA) jednotlivých členských krajín, ktoré v prípade potreby podporujú ďalší bezpečnostní zamestnanci členských krajín. Na zasadnutiach SC sa zúčastňujú zástupcovia Medzinárodného vojenského štábu, Strategických veliteľstiev a výboru C3Board. Zástupcovia civilných a vojenských orgánov NATO môžu byť tiež prítomní, keď budú riešené ich záujmy.

7.3.2. SC zodpovedá priamo NAC za:

(a) preskúmanie Bezpečnostnej politiky NATO (v súlade s C-M(2002)49 a C-M(2002)50) a vypracovanie odporúčaní na zmenu/schválenie zo strany NAC,

(b) preskúmanie otázok týkajúcich sa Bezpečnostnej politiky NATO,

(c) preskúmanie a schvaľovanie podporných smerníc a podporných dokumentov uverejnených SC v oblasti personálnej bezpečnosti, fyzickej bezpečnosti, administratívnej bezpečnosti, priemyselnej bezpečnosti a bezpečnosti CIS (poznámka: krajina môže požiadať o schválenie podpornej smernice aj zo strany NAC), a

(d) posúdenie bezpečnostných záležitostí, na ktoré sa odvoláva NAC, členská krajina, generálny tajomník, vojenský výbor, výbor C3Board alebo vedúci civilných a vojenských orgánov NATO a príprava vhodných odporúčaní.

7.4. **Bezpečnostný úrad NATO (NOS)**

7.4.1. NOS je zriadený v rámci Medzinárodného štábu NATO. Je zložený z personálu so skúsenosťami v bezpečnostných záležitostiach vo vojenskej i civilnej sfére. Úrad udržiava úzku spoluprácu s národnými bezpečnostnými orgánmi (NSA) každej členskej krajiny a civilnými a vojenskými orgánmi NATO. Úrad môže podľa potreby požiadať členské krajiny a civilné a vojenské orgány NATO, aby poskytli dodatočným bezpečnostným odborníkom, aby mu pomáhali na obmedzené časové obdobie, ak by nebolo odôvodnené zamestnať dodatočných pracovníkov na plný úväzok. Riaditeľ NOS je predsedom SC.

7.4.2. NOS je zodpovedný za:

a) preskúmanie akýchkoľvek otázok týkajúcich sa bezpečnosti NATO,

b) identifikovanie prostriedkov, pomocou ktorých by sa mohla zlepšiť bezpečnosť NATO,

(c) celková koordinácia bezpečnosti NATO medzi členskými krajinami a civilnými a vojenskými orgánmi NATO,

(d) zabezpečenie implementácie bezpečnostných rozhodnutí NATO vrátane poskytovania poradenstva, ktoré môžu požadovať členské štáty a civilné a vojenské orgány NATO, a to buď pri uplatňovaní základných zásad a štandardov bezpečnosti popísaných v tejto prílohe, alebo pri realizácii špecifických bezpečnostných požiadaviek,

(e) v prípade potreby informuje SC, generálneho tajomníka a predsedu vojenského výboru o stave bezpečnosti v rámci NATO a pokroku pri implementovaní rozhodnutí NAC týkajúcich sa bezpečnosti,

(f) vykonávanie pravidelných prehliadok bezpečnostných systémov na ochranu utajovaných skutočností NATO v členských krajinách, civilných orgánoch NATO, SHAPE a HQ SACT,

(g) uskutočňovanie pravidelných prehliadok bezpečnostných systémov na ochranu uvoľnených utajovaných skutočností v nečlenských krajinách NATO a medzinárodných organizáciách, s ktorými NATO podpísalo bezpečnostnú dohodu,

(h) koordinácia s národnými bezpečnostnými úradmi a civilnými a vojenskými orgánmi NATO, vyšetrovanie prípadov stratených, zneužitých alebo potenciálne zneužitých utajovaných skutočností NATO,

(i) informovanie národných bezpečnostných úradov o akýchkoľvek informáciách o bezpečnostnom riziku, ktoré sa objavia, pokiaľ ide o ich štátnych príslušníkov,

(j) vypracovanie bezpečnostných opatrení na ochranu ústredia NATO v Bruseli a zabezpečenie ich správnej realizácie, a

(k) vykonávanie úloh, pod vedením a v mene generálneho tajomníka, konajúceho v mene NAC a pod jeho právomocou, zodpovednosti za dohľad nad uplatňovaním bezpečnostného programu NATO na ochranu utajovaných skutočností ATOMAL podľa ustanovení dohody a podporných Administratívnych opatrení, uvedených v bode 3.2 vyššie.

7.5. **Vojenský výbor NATO a vojenské orgány NATO**

7.5.1. Ako najvyšší vojenský orgán v NATO je NAMILCOM zodpovedný za celkové vedenie vojenských záležitostí. NAMILCOM je následne zodpovedný za všetky bezpečnostné záležitosti v rámci vojenskej štruktúry NATO, vrátane centralizovaného celkového rozpoznania opatrení potrebných na zaistenie primeranosti šifrových techník a materiálov používaných na prenos utajovaných skutočností NATO vrátane bezpečnostného schválenia šifrového zariadenia financovaného NATO, ako je definované v prílohe F. V súlade s predtým dohodnutými zásadami a v súlade s jeho referenčným rámcom v odseku 7.4.2 vyššie, NOS vykonáva výkonné funkcie pre bezpečnosť v rámci vojenskej štruktúry NATO a informuje predsedu NAMILCOM.

7.5.2. Vedúci vojenských orgánov NATO zriadených pod záštitou NAMILCOM sú zodpovední za všetky bezpečnostné záležitosti v rámci ich organizácie/útvaru. To zahŕňa zodpovednosť za zabezpečenie zriadenia bezpečnostnej organizácie, vytvorenie a vykonávanie bezpečnostných programov v súlade s Bezpečnostnou politikou NATO a pravidelné kontrolovanie bezpečnostných opatrení na každej veliteľskej úrovni. V prípade organizácií, ktoré sú držiteľmi informácií COSMIC TOP SECRET (CTS) alebo ATOMAL, sa bezpečnostné inšpekcie vykonávajú najmenej raz za 24 mesiacov, pokiaľ počas tejto lehoty inšpekciu nevykoná Bezpečnostný úrad NATO (NOS),

7.6. **Civilné orgány NATO**

7.6.1. Medzinárodný štáb NATO a civilné agentúry NATO sú zodpovedné voči NAC za udržanie bezpečnosti v rámci ich organizácie. To zahŕňa zodpovednosť za zabezpečenie zriadenia bezpečnostnej organizácie, vytvorenie a vykonávanie bezpečnostných programov v súlade s bezpečnostnou politikou NATO a pravidelné kontrolovanie bezpečnostných opatrení na každej veliteľskej úrovni. V prípadoch organizácií, ktoré sú držiteľmi informácií COSMIC TOP SECRET (CTS) alebo ATOMAL,

sa bezpečnostné inšpekcie vykonávajú najmenej raz za 24 mesiacov, pokiaľ nebude v tomto období vykonaná inšpekcia zo strany Bezpečnostného úradu NATO (NOS).

7.7. **Bezpečnosť CIS**

7.7.1. Hlavné organizácie zodpovedné za bezpečnosť CIS (napríklad C3B, NCSAs a NDAs) sú popísané v prílohe F.

8. BEZPEČNOSTNÁ KOORDINÁCIA

8.1. Akýkoľvek bezpečnostný problém NATO, ktorý si vyžaduje koordináciu medzi národnými bezpečnostnými úradmi členských krajín a civilnými a vojenskými orgánmi NATO, bude postúpený Bezpečnostnému úradu NATO (NOS). V prípadoch, keď je takýto prípad postúpený vojenskými orgánmi, uskutoční sa postúpenie informácií prostredníctvom veliteľských kanálov. Akékoľvek nevyriešené rozdiely, ktoré vzniknú v priebehu takejto koordinácie, budú predložené zo strany NOS Bezpečnostnému výboru (SC) na posúdenie.

8.2. Akékoľvek návrhy členských krajín a civilných a vojenských orgánov NATO zahŕňajúce zmeny bezpečnostných postupov NATO sa v prvom rade postúpia NOS. Akékoľvek návrhy vojenských orgánov sa prenášajú prostredníctvom veliteľských kanálov. Ak bezpečnostné problémy NATO, ktoré vedú k takýmto návrhom, nemožno vyriešiť inak ako modifikáciou Bezpečnostnej politiky NATO, budú návrhy postúpené SC a v prípade potreby aj NAC.

Príloha „C“ k
C-M(2002)49

PRÍLOHA „C“

PERSONÁLNA BEZPEČNOSŤ

ÚVOD

1. V tomto dokumente sa stanovujú zásady a minimálne štandardy pre personálnu bezpečnosť. Rozširujúce podrobnosti sa nachádzajú v podpornej smernici o personálnej bezpečnosti.

2. Odsúhlasí sa štandard dôvernosti týkajúci sa lojálnosti, dôveryhodnosti a spoľahlivosti všetkých osôb, ktorým bol udelený prístup k utajovaným skutočnostiam NATO alebo ktorí z titulu svojej funkcie majú prístup k utajovaným skutočnostiam NATO. Všetky osoby, civilné a vojenské, ktorých povinnosti vyžadujú prístup k utajovaným skutočnostiam so stupňom utajenia NC a vyšším, musia byť dostatočne preverené pre zabezpečenie dostatočnej úrovne dôvery, pokiaľ ide o ich spôsobilosť na prístup k takýmto utajovaným skutočnostiam.

3. Osobám oprávneným na oboznamovanie sa s utajovaným skutočnostiam stupňa utajenia NC a vyššie, vydá príslušný národný bezpečnostný úrad alebo iná kompetentná autorita osvedčenie o personálnej bezpečnosti (PSC), ktoré bude platné počas dĺžky trvania oprávneného prístupu, pričom bude zachovaný princíp určenia (Need-to-Know). Rozsah procedúr bezpečnostnej previerky bude závislý od stupňa utajenia utajovaných skutočností NATO, ku ktorým má mať osoba prístup. Princípy bezpečnostnej previerky budú v súlade s bezpečnostnou politikou NATO a doplňujúcimi smernicami.

4. Osobám, ktoré sa potrebujú oboznamovať s utajovanými skutočnosťami stupňa utajenia NC a vyššie, už má byť vystavený príslušný certifikát o personálnej bezpečnosti, pričom tieto osoby musia byť oboznámené s bezpečnostnými postupmi NATO, musia byť tiež oboznámené so svojimi povinnosťami a spĺňajú kritérium určenia (Need-to-know). Osoby, ktoré sa potrebujú oboznamovať s utajovanými skutočnosťami stupňa utajenia NR, sa oboznámia so svojimi bezpečnostnými povinnosťami, pričom tieto musia spĺňať kritérium určenia (Need-to-know). Pokiaľ to národné bezpečnostné pravidlá a predpisy nevyžadujú, bezpečnostná previerka na oprávnenie k oboznamovaniu sa s utajovanými skutočnosťami stupňa utajenia NR nie je potrebná.

5. Vydanie PSC nemožno považovať za konečný krok v procese personálnej bezpečnosti. Aj po vydaní PSC sa naďalej vyžaduje zabezpečenie trvalej spôsobilosti osoby na oboznamovanie sa s utajovanými skutočnosťami NATO. To by sa malo dosahovať prostredníctvom priebežného hodnotenia bezpečnostnými orgánmi a manažérmi; a prostredníctvom bezpečnostného vzdelávania a vzdelávacích programov, ktoré upozornia osoby na ich bezpečnostné povinnosti a potrebu oznamovať svojim riadiacim pracovníkom alebo bezpečnostným štábom informácie, ktoré môžu mať vplyv na ich bezpečnostný status.

UPLATŇOVANIE ZÁSADY „NEED TO KNOW“

6. Osoby z členských štátov NATO a z civilných a vojenských orgánov NATO sa môžu oboznamovať iba s tými utajovanými skutočnosťami NATO, na ktoré majú určenie („Need-to-Know“). Nikto nie je oprávnený na oboznamovanie sa s utajovanými skutočnosťami NATO len na základe svojej funkcie, menovania alebo osvedčenia o personálnej bezpečnosti (PSC).

BEZPEČNOSTNÉ PREVIERKY OSÔB (PSCs):

Zodpovednosti

7. Zodpovednosti národných bezpečnostných úradov alebo iných kompetentných národných autorít, členských štátov NATO a hlavných predstaviteľov civilných alebo vojenských orgánov NATO za PSC, sú uvedené v nariadení o personálnej bezpečnosti.

8. Osoby si majú byť vedomé svojej zodpovednosti konať v súlade s bezpečnostnými predpismi a v záujme bezpečnosti.

Smernica o personálnej bezpečnosti

9. Podporná smernica o personálnej bezpečnosti stanovuje nasledujúce:

(a) požiadavky na identifikáciu pracovných pozícií vyžadujúcich príslušnú PSC,

(b) kritériá na posúdenie lojality, dôveryhodnosti a spoľahlivosti osoby za účelom udelenia a udržania si PSC,

(c) požiadavky na rozsah preverovania pri previerkach stupňa utajenia NATO CONFIDENTIAL, NATO SECRET a COSMIC TOP SECRET,

(d) požiadavky na zabezpečenie PSC pre zamestnancov civilných a vojenských orgánov NATO,

(e) požiadavky na opätovné potvrdenie platnosti PSC,

(f) postupy riešenia bezpečnostného rizika/neoprávnenej manipulácie s utajovanými skutočnosťami o osobe, ktorá je držiteľom PSC, a

(g) požiadavky na vedenie záznamov o PSC udelených osobám.

BEZPEČNOSTNÉ POVEDOMIE A POUČOVANIE OSÔB

10. Všetky osoby zamestnané na pozíciách, v ktorých majú prístup k utajovaným skutočnostiam so stupňom utajenia NR, alebo držitelia osvedčenia o personálnej bezpečnosti pre prístup k utajovaným skutočnostiam so stupňom utajenia NC alebo vyšším, musia byť informovaní o bezpečnostných postupoch a svojich bezpečnostných povinnostiach. Všetky preverené osoby musia potvrdiť, že plne oboznámené so svojimi povinnosťami a dôsledkami, ktoré zákon alebo nariadenie alebo vyhláška ich krajiny upravuje, keď utajované skutočnosti prejdú do neoprávnených

rúk úmyselne alebo z nedbanlivosti. Záznam o potvrdení si ponechá krajina NATO alebo civilný alebo vojenský orgán NATO, ktorý povoľuje prístup k utajovaným skutočnostiam NATO.

11. Všetky osoby oprávnené na oboznamovanie sa s utajovanými skutočnosťami NATO alebo od ktorých sa vyžaduje manipulácia s utajovanými skutočnosťami NATO, musia byť pri nástupe oboznámené a pravidelne preškoľované o hrozbách pre bezpečnosť, ku ktorým môže dôjsť v dôsledku nediskrétnej konverzácie s osobou, ktorá nemá určenie (need-to-know), ich vzťahu s médiami, a hrozbou, ktorú predstavujú aktivity spravodajských služieb zamerané na NATO a jeho členské štáty. Osoby majú byť dôkladne inštruované o týchto nebezpečenstvách a príslušným bezpečnostným autoritám musia okamžite oznámiť akékoľvek snahy alebo manipulácie, ktoré možno považovať za podozrivé alebo nezvyčajné..

OPRÁVNENIE NA PRÍSTUP K UTAJOVANÝM SKUTOČNOSTIAM NATO

PRÍSTUP ŠTÁTNYCH PRÍSLUŠNÍKOV ČLENSKÝCH KRAJÍN NATO

12. Osoba bude mať povolený prístup k utajovaným skutočnostiam NATO len po tom, ako jej bude udelené príslušné osvedčenie o personálnej bezpečnosti, po určení rozsahu na oboznamovanie sa s utajovanými skutočnosťami, a po inštruktáži o bezpečnostných postupoch NATO a oboznámení sa so svojimi bezpečnostné záväzkami.

Výnimočné okolnosti

13. Môžu však nastať okolnosti, keď napríklad pre účely neodkladnej misie, nie je možné splniť niektoré požiadavky uvedené v odseku 12. Podrobnosti týkajúce sa dočasných poverení, jednorazového prístupu, oboznámení sa v krízových situáciách a účasti na konferenciách a stretnutiach sú uvedené v podpornej smernici o personálnej bezpečnosti.

PRÍSTUP ŠTÁTNYCH PRÍSLUŠNÍKOV NEČLENSKÝCH KRAJÍN NATO

14. Štátni príslušníci, ktorí sú z nečlenských krajín NATO a slúžia ako integrovaní členovia ozbrojených síl členov NATO, môžu byť oprávnení na prístup k utajovaným skutočnostiam stupňa utajenia CTS, vrátane. V prípade takýchto štátnych príslušníkov je povinnosťou NSA, aby sa ubezpečil, aby boli splnené podmienky pre prístup, v hore uvedených odsekoch 12 alebo 13.

15. Osobám, ktoré sú štátnymi príslušníkmi [1]nečlenských krajín NATO, môže byť udelený prístup k utajovaným skutočnostiam NATO v jednotlivých prípadoch za predpokladu, že:

1 štátni príslušníci nečlenských krajín NATO zahŕňajú „štátnych príslušníkov kráľovstva“, „občanov štátu“ a „prisťahovalcov na území Kanady“. „Prisťahovalci na území Kanady“ sú osoby, ktoré prešli národným skríningovým procesom vrátane kontroly pobytu, registrov trestov a bezpečnostných kontrol a ktorí idú získať zákonné povolenie na zriadenie trvalého pobytu v krajine.

(a) prístup je potrebný na podporu špecifikovaného programu NATO, projektu, zmluvy, operácie alebo súvisiacej úlohy,

(b) osobe sa udeľuje osobná bezpečnostná previerka (PSC) NATO na základe postupu preverenia, ktoré nie sú menej prísne ako preverenie vyžadované pre štátnych príslušníkov NATO v súlade s Bezpečnostnou politikou NATO a podpornými smernicami, pričom na prístup k utajovaným skutočnostiam stupňa utajenia NATO RESTRICTED sa osvedčenie o personálnej bezpečnosti nevyžaduje,

(c) bol získaný predchádzajúci písomný súhlas krajiny NATO alebo civilného alebo vojenského orgánu NATO, ktorý je pôvodcom utajovanej skutočnosti, a

(d) osoba z nečlenského štátu NATO má svojím podpisom o pochopení svojej zodpovednosti jasne deklarovať, že pochopila a prevzala na seba zodpovednosť za striktné a jediné použitie utajovaných skutočností NATO na účely k zverenej úlohe, ku ktorým bude mať prístup v rámci konkrétneho programu, projektu, kontraktu, operácií alebo súvisiacej úlohe NATO, a tieto utajované skutočnosti nebude zdieľať alebo zasielať tretím osobám, orgánom, organizáciám alebo vládam.

16. Ako výnimku z požiadavky na kontrolu pôvodcu v pododseku 15 (c), môžu národné bezpečnostné úrady krajín NATO schvaľovať prístup k utajovaným skutočnostiam NATO štátnymi príslušníkmi niektorých krajín, ktoré nie sú členmi NATO, ktorí sú zamestnanými vládou krajiny NATO alebo zmluvnou stranou, ktorá má sídlo a je zapísaná do obchodného registra krajiny NATO za predpokladu, že okrem kritérií uvedených v pododsekoch 15 (a), 15 (b) a 15 (d) sa budú uplatňovať kritériá stanovené v ekvivalentnej časti podpornej smernice o personálnej bezpečnosti.

PRÍLOHA „D“ k
C-M(2002)49

PRÍLOHA „D“

FYZICKÁ BEZPEČNOSŤ

ÚVOD

1. V tejto prílohe sa stanovujú zásady a minimálne štandardy pre fyzickú bezpečnosť opatrenia na ochranu utajovaných informácií NATO. Rozširujúce podrobnosti sa nachádzajú v podpornej smernici o fyzickom zabezpečení.

2. Krajiny NATO a civilné a vojenské orgány NATO zavedú programy fyzickej bezpečnosti, ktoré budú spĺňať tieto minimálne štandardy. Takéto programy, ktoré pozostávajú z aktívnych a pasívnych bezpečnostných opatrení, poskytujú spoločný stupeň ochrany utajených skutočností NATO v súlade s ich príslušným stupňom utajenia.

BEZPEČNOSTNÉ POŽIADAVKY

3. Všetky priestory, budovy, kancelárie, miestnosti a iné plochy, v ktorých sa s utajovanými skutočnosťami a materiálmi NATO manipuluje, musia byť chránené primeranými fyzickými bezpečnostnými opatreniami. Pri rozhodovaní o tom, aký stupeň ochrany fyzickej bezpečnosti je potrebný, treba brať do úvahy všetky relevantné faktory, ako napríklad:

(a) stupeň utajenia a kategória informácií,

(b) množstvo a forma informácií (fyzická kópia/uloženie na pamäťovom médiu), ktoré sa uchovávajú,

(c) bezpečnostná previerka personálu a určenie (princíp need-to-know),

(d) lokálne vyhodnotená hrozba zo strany spravodajských služieb, ktorá je zameraná na NATO a/alebo jeho členské krajiny, sabotáž, terorizmus, podvratné alebo iné kriminálne činnosti, a

(e) ako budú utajované skutočnosti uložené.

4. Opatrenia fyzickej bezpečnosti sú navrhnuté tak, aby:

(a) zabránili skrytému alebo násilnému vniknutiu narušiteľa,

(b) odradzovali, bránili a odhaľovali akcie nelojálneho personálu (špióna vo vlastných radoch),

(c) umožnili segregáciu personálu v ich prístupe k utajovaným skutočnostiam NATO v súlade s princípom (need-to-know), a

(d) odhalili a neodkladne riešili všetky bezpečnostné priestupky.

OPATRENIA FYZICKÉJ BEZPEČNOSTI

5. Opatrenia fyzickej bezpečnosti predstavujú len jeden aspekt ochrannej bezpečnosti a musia byť podporené personálnou a administratívnou bezpečnosťou a opatreniami INFOSEC-u, ktorých podrobnosti sa nachádzajú v prílohách C, E a F. Zrozumiteľný manažment bezpečnostných rizík bude zahŕňať stanovenie najefektívnejších a nákladovo najúčinnejších metód boja proti hrozbám a kompenzáciu zraniteľných bodov kombináciou ochranných opatrení z týchto oblastí. Takáto efektívnosť a nákladová účinnosť sa najlepšie dosiahne stanovením požiadaviek na fyzickú bezpečnosť ako súčasť plánovania a navrhovania zariadení, čím sa zníži potreba nákladných renovácií.

6. Programy fyzickej bezpečnosti majú byť založené na princípe hĺbkovej obrany, a hoci opatrenia fyzickej bezpečnosti sú pre každé miesto špecifické, majú platiť nasledujúce všeobecné princípy. V prvom rade je potrebné identifikovať lokality, ktoré vyžadujú ochranu. Nasleduje vytváranie vrstvených bezpečnostných opatrení na zabezpečenie „hĺbkového systému obrany“ a spomaľujúcich prvkov. Vonkajšie opatrenia fyzickej bezpečnosti definujú chránený priestor a zabraňujú neoprávnenému vstupu do chráneného priestoru. Ďalšia úroveň opatrení rozpozná neoprávnený vstup alebo snahu o vstup a upozorní strážnu službu. Vnútorná úroveň opatrení má dostatočne zdržať narušiteľov, až do chvíle ich zadržania strážnou službou. V dôsledku toho existuje vzájomný vzťah medzi reakčným časom strážnej služby a opatreniami fyzickej bezpečnosti vytvorenými na zdržanie narušiteľov.

7. Pravidelná údržba bezpečnostných systémov je nevyhnutná na zabezpečenie optimálneho výkonu zariadení. Tiež je potrebné pravidelne prehodnocovať účinnosť jednotlivých bezpečnostných opatrení a celého bezpečnostného systému. Toto je obzvlášť dôležité, ak dôjde k zmene používania lokality alebo prvkov bezpečnostného systému. To možno dosiahnuť uplatnením plánov reakcie na incidenty.

Chránený priestor

8. Priestory, v ktorých sa spracúvajú a uchovávajú utajované skutočnosti so stupňom utajenia NC a vyšším, sa organizujú a štruktúrujú tak, aby zodpovedali jednému z nasledujúcich:

a) **Chránený priestor NATO triedy I**: oblasť, v ktorej sa spracúvajú a ukladajú utajované skutočnosti so stupňom utajenia NC a vyšším, a to takým spôsobom, že vstup do oblasti predstavuje pre všetky praktické účely prístup k utajovaným skutočnostiam. Takáto oblasť si vyžaduje:

(i) jasne definovaný a chránený obmedzený priestor, cez ktorý sa kontroluje každý vstup a výstup,

(ii) systém kontroly vstupu, ktorý povolí vstup len tým osobám, ktoré boli riadne preverené a majú osobitné oprávnenie na vstup do oblasti,

(iii) špecifikácia stupňa utajenia a kategórie informácií zvyčajne uložených v oblasti, t. j. informácie, ku ktorým je umožnený prístup vstupom do oblasti,

b) **Chránený priestor NATO triedy II**: oblasť, v ktorej sa spracúvajú a ukladajú utajované skutočnosti so stupňom utajenia NC a vyšším, a to takým spôsobom, že môžu byť chránené voči prístupu nepovolaných osôb vnútorne zriadenými kontrolami. Takáto oblasť si vyžaduje:

i) jasne definovaný a chránený obmedzený priestor, cez ktorý sa kontroluje každý vstup a výstup,

ii) systém kontroly vstupu, ktorý umožní vstup bez sprievodu len tým osobám, ktoré sú bezpečnostne preverené a majú osobitné oprávnenie pre vstup do oblasti. Pri všetkých ostatných osobách musí byť zabezpečený sprievod alebo zodpovedajúca kontrola, aby sa zabránilo neoprávnenému prístupu k utajovaným skutočnostiam NATO a nekontrolovanému vstupu do priestorov podliehajúcich technickej bezpečnostnej kontrole.

9. Tie oblasti, v ktorých sa nenachádza službukonajúci personál 24 hodín denne, sa kontrolujú okamžite po skončení bežnej pracovnej doby, aby sa zabezpečilo, že utajované skutočnosti NATO sú riadne zabezpečené.

Administratívne zóny

10. Administratívna zóna môže byť vytvorená okolo chránených priestorov NATO I. alebo II. triedy. Takáto zóna vyžaduje viditeľne definovanú hranicu, v rámci ktorej existuje možnosť kontroly osôb a vozidiel. V administratívnych zónach sa budú spracúvať a uchovávať iba utajované skutočnosti do stupňa utajenia NR vrátane.

Prístup do chránených priestorov NATO II. triedy osobami z nečlenských krajín NATO/medzinárodných organizácií

11. Osoby z nečlenských krajín NATO/medzinárodných organizácií, ktoré z dôvodu svojho poverenia, potrebujú byť v pravidelnom styku s pracovníkmi NATO, môžu získať oprávnenie na vstup bez sprievodu do chráneného priestoru NATO II. triedy. Takýmto osobám môžu byť pridelené kancelárske priestory v rámci chráneného priestoru NATO II. triedy, za účelom plnenia svojich úloh a služobných povinností. Udelenie vstupu bez sprievodu a/alebo pridelenie kancelárskych priestorov sa rieši individuálnym posúdením a je v súlade s kritériami stanovenými v podpornej smernici o fyzickej bezpečnosti.

Špecifické opatrenia

12. Nasledujúce opatrenia sú určené na označenie príkladov opatrení fyzickej bezpečnosti, ktoré môžu byť implementované:

(a) oplotenie obmedzeného priestoru - oplotenie bude tvoriť užitočnú fyzickú bariéru a identifikuje hranicu oblasti vyžadujúcej bezpečnostnú ochranu. Účinnosť bezpečnostného obmedzeného priestoru bude vo veľkej miere závisieť od úrovne bezpečnosti v miestach prístupu,

(b) elektronický zabezpečovací systém (ESZ) – ESZ môže byť použitý na obmedzených priestoroch na zvýšenie úrovne zabezpečenia, ktorú poskytuje oplotenie alebo môže byť použitý v miestnostiach a budovách namiesto alebo v rámci asistencie strážnym zložkám,

(c) kontrola vstupu – kontrola vstupu sa môže vykonávať na mieste, v budove alebo budovách v lokalite alebo v priestoroch alebo miestnostiach v rámci budovy. Kontrola môže byť elektronická, elektromechanická, strážcom alebo recepčným alebo fyzická,

(d) strážna služba - zamestnanie primerane preverených, vyškolených a kontrolovanej strážnej služby môže poskytnúť hodnotný odstrašujúci prostriedok voči osobám, ktoré by mohli plánovať skryté narušenie,

(e) uzavretý televízny okruh (CCTV) - CCTV je hodnotná pomôcka strážnej služby pri overovaní incidentov a alarmov ESZ v rozľahlých lokalitách alebo obmedzených priestoroch, a

(f) bezpečnostné osvetlenie - bezpečnostné osvetlenie môže predstavovať pre potenciálneho narušiteľa vysoký stupeň odstrašenia okrem toho, že poskytuje osvetlenie potrebné pre účinné pozorovanie buď priamo strážnou službou, alebo nepriamo prostredníctvom systému CCTV.

Vstupné a výstupné prehliadky

13. Orgány NATO vykonávajú náhodné vstupné a výstupné prehliadky, ktoré sú navrhnuté tak, aby pôsobili ako odstrašujúci prostriedok proti neoprávnenému noseniu materiálu alebo neoprávnenému vynášaniu utajovaných skutočností NATO z lokality alebo budovy.

Kontrola vstupu

14. Na kontrolu vstupu každodenného personálu do chránených priestorov NATO triedy I. alebo II, má byť zavedený systém vstupu alebo rozpoznania osoby. Návštevníkom sa umožní vstup do priestorov NATO v sprievode alebo bez sprievodu, ktorý bude založený na prehliadkach jednotlivcov a ich požiadaviek na vstup. ***December 2006***

PRÍLOHA „D“ k
C-M(2002)49

MINIMÁLNE ŠTANDARDY NA UKLADANIE UTAJOVANÝCH SKUTOČNOSTÍ NATO

15. Utajované skutočnosti NATO sa budú uschovávajú len v podmienkach, ´vytvorených na zabránenie a odhalenie neoprávneného prístupu k nim.

16. **COSMIC TOP SECRET (CTS)**. Utajované skutočnosti CTS sa uchovávajú v rámci chráneného priestoru I. alebo II. triedy za jednej z nasledujúcich podmienok:

(a) v trezore vybavenom ESZ alebo v oficiálne schválenom bezpečnostnom kontajneri danej krajiny, ktorý podlieha nepretržitej ochrane alebo pravidelnej kontrole, alebo

(b) otvorený skladovací priestor s ochranou ESZ postavený v súlade s podpornou smernicou o fyzickej bezpečnosti.

17. **NATO SECRET (NS).** Utajované skutočnosti so stupňom utajenia NS sa musia ukladať v chránenej oblasti I. a II. triedy za jednej z nasledujúcich podmienok:

a) rovnakým spôsobom, ako je predpísané pre utajované skutočnosti CTS, alebo

b) v oficiálne schválenom bezpečnostnom kontajneri danej krajiny alebo trezore, alebo

(c) otvorenom skladovacom priestore, ktorý je chránený ESZ alebo podlieha nepretržitej ochrane alebo pravidelnej kontrole.

18. **NATO CONFIDENTIAL (NC).** Utajované skutočnosti so stupňom ochrany NC sa ukladajú rovnakým spôsobom, ako je predpísané pre utajované skutočnosti so stupňom ochrany CTS alebo NS, s výnimkou toho, že sa nevyžadujú doplnkové kontroly, ako sú opísané v podpornej smernici o fyzickej bezpečnosti.

19. **NATO RESTRICTED (NR).** Utajované skutočnosti NR sa musia ukladať v uzamknutom kontajneri.

20. Ďalšie podrobnosti o ukladaní utajovaných skutočností NATO sú uvedené v podpornej smernici o fyzickej bezpečnosti.

OCHRANA PROTI TECHNICKÝM ÚTOKOM

Odpočúvanie

21. Kancelárie alebo priestory, v ktorých sa pravidelne prerokúvajú utajované skutočnosti so stupňom utajenia NS a vyšším, musia byť chránené útokom pasívneho a aktívneho odpočúvania prostredníctvom dôkladných fyzických zabezpečovacích opatrení a kontroly vstupu, v závislosti od výskytu rizika. Zodpovednosť za určenie výšky rizika sa koordinuje s technickými odborníkmi a rozhodne o tom príslušný bezpečnostný orgán.

Technicky zabezpečené priestory

22. Priestory, ktoré sa majú chrániť pred odpočúvaním, sa označujú ako technicky zabezpečené priestory a vstup do nich musí byť osobitne kontrolovaný. Miestnosti musia byť uzamknuté a/alebo strážené v súlade so štandardami fyzickej bezpečnosti, ak nie sú obsadené a s akýmikoľvek kľúčmi sa musí zaobchádzať ako s bezpečnostnými kľúčmi. Takéto priestory podliehajú pravidelným fyzickým a/alebo technickým kontrolám v súlade s požiadavkami príslušného bezpečnostného orgánu a vykonávajú sa aj po akomkoľvek neoprávnenom vstupe alebo podozrení na takýto vstup a pri vstupe externých pracovníkov za účelom údržbárskych prác alebo rekonštrukcie.

FYZICKÉ ZABEZPEČENIE KOMUNIKAČNÝCH A INFORMAČNÝCH SYSTÉMOV (CIS)

23. Priestory, v ktorých sa utajované skutočnosti NATO prerokúvajú alebo sa s nimi manipuluje s použitím informačných technológií alebo kde je možný prístup k takýmto utajovaným skutočnostiam, sa zabezpečia tak, aby bola splnená súhrnná požiadavka na dôvernosť, integritu a dostupnosť. Oblasti, v ktorých sa používajú CIS na zobrazovanie, ukladanie, spracovanie alebo prenos utajovaných skutočností so stupňom utajenia NC a vyšším alebo kde je možný prístup k takýmto utajovaným skutočnostiam, sa zabezpečia ako chránený priestor NATO I. a II. triedy alebo ekvivalent v príslušnej krajine. Priestory, v ktorých sa používajú CIS na zobrazovanie, ukladanie, spracovanie alebo prenos utajovaných skutočností so stupňom utajenia NR, alebo kde je možný prístup k takýmto utajovaným skutočnostiam, sa môžu zabezpečiť ako administratívne zóny.

SCHVÁLENÉ ZARIADENIE

24. Národné bezpečnostné úrady vedú zoznamy zariadení, ktoré oni alebo iné krajiny NATO schválili na ochranu utajovaných skutočností NATO pre rôzne špecifické okolnosti a podmienky. Civilné a vojenské orgány NATO zabezpečia, aby akékoľvek zakúpené zariadenie vyhovovalo predpisom členského štátu (štátov) NATO.

OSTATNÉ OPATRENIA FYZICKÉHO ZABEZPEČENIA

25. Podrobné požiadavky sú vymedzené v podpornej smernici o fyzickej bezpečnosti, ktorá sa týka napríklad miestností a zámkov, kľúčov a kombinácií, úschovných kontajnerov a ich zámkov.

PRÍLOHA „E“ k
C-M(2002)49

PRÍLOHA „E“

ADMINISTRATÍVNA BEZPEČNOSŤ

ÚVOD

1. V tomto dokumente sa stanovujú zásady a minimálne štandardy pre bezpečnosť utajovaných skutočností NATO. Rozširujúce podrobnosti sa nachádzajú v podpornej smernici o administratívnej bezpečnosti.

2. Utajované skutočnosti NATO si vyžadujú ochranu počas ich celého životného cyklu. Zabezpečí sa ich primerané utajenie, zreteľné označenie ako utajovaných skutočností a dĺžka ich utajenia len na nevyhnutne potrebné obdobie. Opatrenia administratívnej bezpečnosti budú doplnené opatreniami o personálnej bezpečnosti a INFOSEC-om s cieľom zabezpečiť vyvážený systém úbor opatrení na ochranu utajovaných skutočností NATO.

STUPEŇ UTAJENIA a OZNAČENIA

Všeobecne

3. Pôvodca je zodpovedný za stanovenie stupňa utajenia a prvotnú distribúciu utajovanej skutočnosti. Stupeň utajenia utajovanej skutočnosti NATO sa nezmení alebo nezníži, resp. utajovaná informácia nebude odtajnená bez súhlasu pôvodcu. V čase jej vytvorenia, má pôvodca tam, kde je to možné, uviesť, či je možné znížiť jej stupeň utajenia alebo či ju je možné po určitom čase alebo určitej udalosti úplne odtajniť.

4. Pridelený stupeň utajenia určuje úroveň fyzickej ochrany, ktorá je utajovanej skutočnosti poskytnutá pri jej úschove, prenose, obehu a zničení a zároveň udáva stupeň bezpečnostnej previerky personálu, ktorý sa má s ňou oboznamovať. V záujme účinného zabezpečenia utajovaných skutočností a zároveň efektívnosti by sa mali zamedziť nadhodnocovaniu alebo podhodnocovaniu ich stupňa utajenia. Určený stupeň zabezpečenia určuje fyzické zabezpečenie informácií pri skladovaní a prenose, ich obehu, zničení a bezpečnostnej previerke personálu požadovanej pre prístup. Preto by sa malo predchádzať tak nadmernému stupňu utajenia ako aj nedostatočnému stupňu utajenia v záujme účinného zabezpečenia a efektívnosti.

5. Krajiny NATO a civilné a vojenské orgány NATO zavedú opatrenia, ktorými zabezpečia, aby utajované skutočnosti vytvorené NATO alebo poskytnuté NATO mali správny stupeň utajenia a boli chránené v súlade s požiadavkami smernice o administratívnej bezpečnosti.

6. Každý civilný alebo vojenský orgán NATO má vytvoriť systém na zabezpečenie pravidelného prehodnocovania utajovaných skutočností stupňa utajenia CTS, ktorých je pôvodcom, minimálne raz za päť rokov, aby sa zistilo, či dôvody pridelenia stupňa utajenie CTS naďalej pretrvávajú. Takéto prehodnocovanie nie je potrebné v tých prípadoch, kde pôvodca vopred stanovil, že jednotlivým utajovaným skutočnostiam stupňa utajenia CTS bude po dvoch rokoch automaticky znížený stupeň utajenia a utajované skutočnosti boli takto označené.

7. Celkový stupeň utajenia dokumentu má byť minimálne totožný so stupňom utajenia dokumentu s najvyšším stupňom utajenia. Jednotlivé časti dokumentov so stupňom utajenia NC a vyšším sa podľa možnosti klasifikujú (vrátane podľa odseku) podľa pôvodcu s cieľom uľahčiť rozhodovanie o ďalšom šírení príslušných odsekov. Sprievodné dokumenty musia byť označené príslušným stupňom utajenia utajovaných skutočností v nich obsiahnutých, v prípade, ak sa od utajovanej skutočnosti oddelia.

8. Pokiaľ bude utajovaná skutočnosť vytváraná z viacerých zdrojov, bude posúdený aj stupeň utajenia výslednej utajovanej skutočnosti, nakoľko môže byť vyšší než stupne utajenia jej jednotlivých častí. Pôvodné označenia stupňov utajenia, keď sa utajovaná skutočnosť používa na prípravu súhrnných dokumentov, musia zostať zachované. Ak sa zhromaždia informácie z rôznych zdrojov, produkt sa preskúma

Označenia stupňa utajenia

9. Pojmy COSMIC a NATO sú označenia stupňa utajenia, ktoré pri použití na utajované skutočnosti znamenajú, že utajované skutočnosti sú chránené v súlade s Bezpečnostnou politikou NATO.

Označenia špeciálnej kategórie

10. Pojem „ATOMAL“ je označenie, ktoré sa používa na označenie špeciálnej kategórie utajovaných skutočností, čo znamená, že tieto utajované skutočnosti musia byť chránené v súlade s dohodou a podpornými administratívnymi opatreniami uvedenými v prílohe B, odsek 5.

11. Pojem „SIOP“ je označenie, ktoré sa používa na označenie špeciálnej kategórie utajovaných skutočností, čo znamená, že tieto utajované skutočnosti musia byť chránené v súlade s odkazom v prílohe B, odsek 6.

12. Pojem „CRYPTO“ je označenie a kvalifikátor osobitnej kategórie, ktoré identifikuje všetky kľúčové materiály COMSEC-u, ktoré sa používajú na ochranu alebo overenie telekomunikačných služieb, ktoré obsahujú utajované skutočnosti súvisiace s bezpečnosťou NATO, čo znamená, že utajované skutočnosti sú chránené v súlade s príslušnými šifrovými bezpečnostnými pokynmi.

13. Termín „BOHEMIA“ je označenie, ktoré sa vzťahuje na špeciálnu kategóriu utajovaných skutočností pochádzajúcich alebo týkajúcich sa komunikačných spravodajských utajovaných skutočností (COMINT). Všetky utajované skutočnosti označené COSMIC TOP SECRET - BOHEMIA budú chránené v prísnom súlade s politikou MC 101 (NATO Signals Inteliligence Policy) a s jej príručkou Spoločnou spojeneckou publikáciou (AJP), ktorá pokrýva doktrinálne a procedurálne otázky

Označenie na obmedzenie šírenia

14. Ako doplňujúce označenie na ďalšie obmedzenie šírenia utajovaných skutočností NATO môže pôvodca používať značku obmedzenia šírenia.

KONTROLA A MANIPULÁCIA

Ciele účtovateľnosti

15. Hlavným cieľom zodpovednosti je zabezpečovať dostatočné informácie potrebné na prešetrovanie zámerného alebo náhodného zneužitia účtovateľných utajovaných skutočností a zhodnotenie škody, ktorá vznikne ich zneužitím. Požiadavka na účtovateľnosť slúži na zavedenie disciplíny pri manipulácii a kontrole prístupu k účtovateľným utajovaným skutočnostiam.

16. Vedľajšie ciele sú:

(a) viesť záznamy o prístupoch k účtovateľným utajovaným skutočnostiam - kto mal alebo eventuálne môže mať prístup k účtovateľným utajovaným informáciám, a kto sa pokúšal dostať k účtovateľným utajovaným skutočnostiam,

(b) vedieť lokalizovať účtovateľné utajované skutočnosti , a

(c) viesť záznamy o pohybe účtovateľných utajovaných skutočností v rámci NATO a národných domén.

17. Utajované skutočnosti CTS, NS a ATOMAL majú byť účtovateľnými utajovanými skutočnosťami, majú sa kontrolovať a spracovávať v súlade s požiadavkami tejto prílohy a doplňujúcou smernicou o administratívnej bezpečnosti. Tam, kde to národné pravidlá a predpisy požadujú, utajované skutočnosti, ktoré nesú inú bezpečnostnú klasifikáciu alebo označenia špeciálnej kategórie, sa môžu považovať za účtovateľné utajené skutočnosti.

Systém registrov

18. Systém registrov je zodpovedný za príjem, účtovanie, manipuláciu, distribúciu a ničenie účtovateľných utajovaných skutočností. Táto zodpovednosť sa môže plniť buď v rámci jedného systému registra, pričom v takomto prípade sa vždy dodržiava prísne oddelenie utajovaných skutočností CTS alebo zriadením oddelených registrov a kontrolných bodov.

19. Každá členská krajina NATO a civilný alebo vojenský orgán NATO zriadia centrálny register (registre) pre CTS, ktorý je hlavným prijímajúcim a odosielajúcim orgánom krajiny alebo orgán, v ktorom bol založený. Centrálny register (registre) môže tiež pôsobiť ako register (registre) pre ostatné účtovateľné utajované skutočnosti.

20. Registre a kontrolné body pôsobia ako zodpovedná organizácia pre vnútornú distribúciu utajovaných skutočností CTS a NS a za vedenie záznamov o všetkých účtovateľných utajovaných skutočnostiach vedených na tomto registri alebo kontrolnom bode, môžu sa zriadiť na ministerstve, oddelení alebo na rôznych úrovniach velenia.

Nevyžaduje sa, aby boli utajované skutočnosti NC a NR spracovávané prostredníctvom systému registra, pokiaľ to nie je určené národnými bezpečnostnými pravidlami a predpismi.

21. Pokiaľ ide o účtovateľné utajované skutočnosti NATO, musia byť registre a kontrolné body schopné vždy stanoviť miesto svojho založenia. Zriedkavý a dočasný prístup k takýmto utajovaným skutočnostiam si nevyžaduje nevyhnutné zriadenie registra alebo kontrolného bodu za predpokladu, že existujú postupy na zabezpečenie, aby utajované skutočnosti zostali pod kontrolou systému registra.

22. Šírenie utajovaných skutočností so stupňom utajenia CTS sa uskutočňuje prostredníctvom kanálov registra COSMIC. Najmenej raz ročne uskutoční každý register vykoná súpis všetkých utajovaných skutočností so stupňom utajenia CTS, za ktoré je zodpovedný, v súlade s požiadavkami podpornej Smernice o administratívnej bezpečnosti. Bez ohľadu na typ organizácie registrov, tie, ktoré manipulujú s utajovanými skutočnosťami so stupňom utajenia CTS, vymenujú funkciu „COSMIC Control Officer“ (CCO).

23. V podpornej smernici o administratívnej bezpečnosti sa okrem iného stanovujú povinnosti CCO, podrobné postupy manipulácie systému registra pre utajované skutočnosti CTS a NS, postupy reprodukcie, preklady a výpisy, požiadavky na šírenie prenosu utajovaných skutočností a požiadavky na likvidáciu a zničenie utajovaných skutočností.

24. NAMILCOM zaviedol samostatný systém pre zodpovednosť, kontrolu a distribúciu šifrového materiálu. Materiál, ktorý sa prenáša cez tento systém, nevyžaduje sledovateľnosť zodpovednosti v systéme registrov.

NÚDZOVÉ PLÁNOVANIE

25. Krajiny NATO a civilné a vojenské orgány NATO pripravia núdzové plány na ochranu alebo zničenie utajovaných skutočností NATO v núdzových situáciách s cieľom zabrániť neoprávnenému prístupu a odhaleniu a strate ich dostupnosti. Tieto plány dávajú najvyššiu prioritu najcitlivejším, najdôležitejším utajovaným skutočnostiam pre úspešnosť misie.

BEZPEČNOSTNÉ PRIESTUPKY A ZNEUŽITIE

26. Ochrana utajovaných skutočností NATO závisí od návrhu vhodných bezpečnostných predpisov na vykonanie schválenej bezpečnostnej politiky, smerníc a nariadení a od účinného vykonávania týchto predpisov prostredníctvom školení a kontroly dodržiavania, podporenej disciplinárnymi a v krajných prípadoch aj právnymi sankciami.

27. Všetky prípady porušenia bezpečnosti sa okamžite oznámia príslušnému bezpečnostnému orgánu. Každé hlásené porušenia bezpečnosti prešetria osoby, ktoré majú bezpečnostné, vyšetrovacie a, ak je to potrebné, skúsenosti z kontrarozviedky a sú nezávislé od osôb, ktorých sa porušenie bezprostredne týka.

28. Hlavným účelom ohlasovania zneužitia utajovaných skutočností NATO je umožniť, aby pôvodca (zložka NATO) posúdil vzniknuté škody pre NATO a podnikol akékoľvek kroky, ktoré sú žiaduce alebo uskutočniteľné na minimalizovanie škôd. Hlásenia o posúdení škôd a minimalizácia prijatých opatrení sa postúpia na NOS.

29. Ak musí byť NOS oznámené zneužitie / neoprávnená manipulácia s utajovanými skutočnosťami NATO, hlásenie sa odosiela prostredníctvom NSA alebo vedúceho príslušného civilného alebo vojenského orgánu NATO. Ak je to možné, ohlasujúci orgán musí informovať pôvodcu NATO súčasne s NOS. NOS však môže byť zároveň požiadaný, aby to urobil v prípadoch, keď je zložité určiť pôvodcu utajovanej skutočnosti. Načasovanie hlásení závisí od citlivosti utajovaných skutočností a okolností.

30. Generálny tajomník NATO môže požiadať príslušné orgány, aby vykonali ďalšie prešetrovania a o výsledku šetrenia podali správu.

31. Podporná smernica o administratívnej bezpečnosti stanovuje podrobné opatrenia, záznamy a požiadavky na podávanie správ o porušeniach a zneužitiach bezpečnosti.

32. Samostatné ustanovenia týkajúce sa narušenia šifrového materiálu boli vydané zo strany NAMILCOM pre komunikáciu bezpečnostných orgánov členských krajín a civilných a vojenských orgánov NATO.

BEZPEČNOSTNÉ OPATRENIA NA UVOĽNENIE UTAJOVANÝCH SKUTOČNOSTÍ DO NEČLENSKÝCH KRAJÍN NATO A MEDZINÁRODNÝCH ORGANIZÁCIÍ

Úvod

33. Utajované skutočnosti, ktoré sú zverené alebo vytvorené NATO na to, aby mohli plniť svoje poslanie, musia byť šírené a chránené v súlade s Bezpečnostnou politikou NATO, smernicami a postupmi. Táto časť stanovuje politiku uvoľňovania utajovaných skutočností NATO do krajín, ktoré nie sú členmi NATO a medzinárodných organizácií vrátane takýchto krajín (ďalej len „príjemcovia mimo NATO“). Táto časť sa vzťahuje aj na utajované skutočnosti obsiahnuté v dokumentoch vydaných NAC alebo akýmkoľvek iným výborom NATO alebo civilným alebo vojenským orgánom NATO (ďalej len „orgány NATO“).

34. Uvoľnenie utajovaných skutočností NATO príjemcom, ktorí sú mimo NATO, sa uskutoční v rámci medzinárodnej spolupráce schválenej NAC. Každá žiadosť o uvoľnenie utajovaných skutočností NATO príjemcom, ktorí nie sú členmi NATO, mimo takýchto činností spolupráce, sa musí preskúmať a schváliť od prípadu k prípadu.

35. Utajované skutočnosti ATOMAL akéhokoľvek stupňa utajenia nesmú byť uvoľnené žiadnej krajine/organizácii, ktorá nie je signatárom súčasných verzií CM(64)39 a CM(68)41.

PRÍLOHA „E“ k
C-M(2002)49

Zásady uvoľňovania vydania utajovaných skutočností NATO do nečlenských krajín NATO a medzinárodných organizácií

36. Oprávnenie na uvoľnenie bude vždy podliehať súhlasu pôvodcu(-ov). Okrem toho bude platiť nasledovné:

(a) pre utajované skutočnosti NATO, ktoré majú byť postúpené na základe medzinárodnej spolupráce NATO schválenej v NAC, kde účastníci mimo NATO tohto postúpenia boli schválení v NAC na základe posúdenia od prípadu k prípadu:

(i) rozhodnutia o uvoľnení sa môžu týkať buď jasne určených informácií, alebo všeobecnej kategórie informácií,

(ii) predmetná záležitosť bude zahrnutá do všeobecného pracovného plánu pre činnosť alebo do aktivít OPLAN alebo do praktických opatrení, stanovených pre spoluprácu,

(iii) uvoľnenie utajovaných skutočností NATO je nevyhnutné na začatie spolupráce v konkrétnej veci a na pokračovanie spolupráce v rámci už schválenej činnosti,

(iv) musí byť uzavretá bezpečnostná dohoda podpísaná generálnym tajomníkom v mene NATO a riadne povereným zástupcom [2] nečlenských krajín NATO. Ak neexistuje bezpečnostná dohoda a za výnimočných okolností, s cieľom podporiť špecifické prevádzkové požiadavky schválené NAMILCOM/NAC (napríklad na podporu ochrany síl a výmenu spravodajských utajovaných skutočností) príjemca z nečlenskej krajiny NATO, podpísaný svojím riadne povereným[1] zástupcom poskytne NOS bezpečnostnú záruku, že akékoľvek získané utajované skutočnosti budú chránené v súlade so zákonmi a predpismi krajiny a spôsobom, ktorý nie je menej prísny ako minimálne štandardy NATO,

(v) ak je s medzinárodnou organizáciou uzavretá bezpečnostná dohoda, uvoľnenie utajovaných skutočností jej členom, ktorí nie sú členmi NATO, musí byť v súlade s príslušnými ustanoveniami bezpečnostnej dohody, ako aj ďalšími ustanovenými pravidlami týkajúcimi sa ich účasti na aktivitách NATO,

(vi) bezpečnostná záruka poskytnutá príjemcovi, ktorý nie je členom NATO, musí tiež obsahovať identifikáciu stupňov utajenia NATO a ekvivalentných stupňov utajenia príjemcu z nečlenskej krajiny NATO. Bezpečnostná záruka sa zašle príslušnému výboru zodpovednému za schválenie uvoľnenia.

[2] „Riadne poverený zástupca“ je oficiálne poverený zástupca, ktorý je buď priamym príjemcom uvoľnených utajovaných informácií, alebo je vyšším zástupcom zodpovedným za zabezpečenie ochrany utajovaných skutočností poskytnutých na podporu spoločnej činnosti“.

Kópie písomnej bezpečnostnej záruky sa poskytujú Bezpečnostnému úradu NATO, ktorý vedie databázu bezpečnostných záruk,

(vii) iba utajované skutočnosti do stupňa utajenia NC vrátane, môžu byť uvoľnené na základe bezpečnostných záruk. Za výnimočných okolností však môžu byť utajované skutočnosti NS uvoľnené vydané za účelom podpory špecifických operačných požiadaviek schválených zo strany NAMILCOM/NAC, a

(viii) ak existuje požiadavka na sprístupnenie utajovaných skutočností NS nečlenskej krajine NATO, ktorá podpísala bezpečnostnú dohodu so sponzorom NATO, sponzor NATO poskytne potrebné záruky, že existuje príslušný bezpečnostný systém na ochranu takýchto uvoľnených utajovaných skutočností a požiada o schválenie uvoľnenia utajovaných skutočností ešte pred ich uvoľnením, a

(b) pre utajované skutočnosti NATO, ktoré majú byť vydané na základe osobitnej žiadosti zo strany členských krajín NATO (sponzor) pre príjemcov z nečlenských krajín NATO mimo kooperačných aktivít schválených NAC:

(i) rozhodnutia o uvoľnení sa vykonávajú na základe individuálneho posúdenia a môžu sa týkať len jasne identifikovaných informácií,

(ii) medzi členskou krajinou NATO sponzorujúcou uvoľnenie a príjemcom mimo NATO musí existovať bilaterálna bezpečnostná dohoda,

(iii) sponzor zodpovedá za poskytnutie písomnej bezpečnostnej záruky pre NATO od príjemcu mimo NATO, ktorú podpíše riadne poverený[3] zástupca príjemcu mimo NATO s právoplatným mandátom. Bezpečnostná záruka, ktorú poskytne príjemca NATO, príjemcu mimo NATO zaväzuje chrániť utajované skutočnosti NATO minimálne na taký stupeň, aký obsahujú ustanovenia bilaterálnej bezpečnostnej dohody / opatrenia na ochranu utajovaných skutočností sponzora. K stupňom utajenia NATO sa identifikujú ekvivalenty stupňov utajenia národných utajovaných skutočností, ktoré sa uvedú v bilaterálnej bezpečnostnej dohode / opatrení,

[3] „„Riadne poverený zástupca“ je oficiálne poverený zástupca, ktorý je buď priamym príjemcom uvoľnených utajovaných informácií, alebo je vyšším zástupcom zodpovedným za zabezpečenie ochrany utajovaných skutočností poskytnutých na podporu spoločnej činnosti“.

(iv) sponzor predloží túto písomnú bezpečnostnú záruku príslušnému výboru spolu so žiadosťou o uvoľnenie. Kópia písomných bezpečnostných záruk sa poskytne aj NOS,

(v) požiadavka má poukázať na výhodu, ktorá NATO môže vzniknúť. Odôvodnenia na uvoľnenie majú byť konkrétne, má sa vyhnúť všeobecným prehláseniam,

(vi) ak je s medzinárodnou organizáciou uzavretá bezpečnostná dohoda, uvoľnenie informácií jej členom, ktorí nie sú členmi NATO, musí byť v súlade s príslušnými ustanoveniami bezpečnostnej dohody, ako aj ďalšími ustanovenými pravidlami týkajúcimi sa ich účasti na aktivitách NATO, a

(vii) iba utajované skutočnosti so stupňom utajenia do NC vrátane môžu byť v tomto prípade vydané na základe bezpečnostných záruk. Ak existuje požiadavka na sprístupnenie utajovaných skutočností NS nečlenskej krajine NATO, ktorá podpísala bezpečnostnú dohodu so sponzorom NATO, sponzor NATO poskytne potrebné záruky, že existuje príslušný bezpečnostný systém na ochranu takýchto uvoľnených utajovaných skutočností a požiada o súhlas príslušného výboru zodpovedného za schválenie uvoľnenia pred ich uvoľnením.

Orgán zodpovedný za uvoľňovanie utajovaných skutočností

37. NAC disponuje ultimátnou právomocou na uvoľnenie utajovaných informácií NATO príjemcom z nečlenských krajín NATO. Tento orgán dodržiava princíp súhlasu pôvodcu a v súlade s princípmi oprávnenia na uvoľnenie uvedené v odseku 36 vyššie, deleguje svoje právomoci na:

(a) príslušný predmetný výbor pre utajované skutočnosti so stupňom utajenia až do NS vrátane, ktorých pôvodca je tento výbor a/alebo jemu podriadené orgány. V prípade utajovaných skutočností NR môže vecne príslušný výbor ďalej delegovať svoje právomoci na jasne určenú funkciu podporného personálu alebo na konkrétnu úlohu v rámci podporného personálu tohto výboru,

(b) NAMILCOM pre utajované skutočnosti so stupňom utajenia až do NS vrátane, ktorých pôvodca je NAMILCOM a/alebo jemu podriadené orgány. V prípade utajovaných skutočností NR môže NAMILCOM ďalej delegovať právomoc na jasne identifikovanú funkciu podporného personálu alebo na konkrétnu úlohu v rámci podporného personálu NAMILCOM,

(c) SACEUR alebo D/SACEUR pre utajované skutočnosti so stupňom utajenia do NS vrátane, ktoré sú označené ako tie, ktoré sa môžu uvoľniť pre xFOR, alebo je so stupňom utajenia NATO/xFOR SECRET (misia SECRET) za týchto podmienok:

(i) utajované skutočnosti sú obmedzené na utajované skutočnosti NATO nevyhnutné na efektívnu účasť nečlenských krajín NATO, ktoré poskytujú svoj kontingent vojsk (NNTCN) pri operáciách a cvičeniach, na základe individuálneho schválenia NAC,

(ii) utajované skutočnosti , ktoré majú byť uvoľnené, sú iba tie utajované skutočnosti NATO, ktoré vznikli v rámci Spojeneckého veliteľstva pre operácie (ACO) a priamo súvisia so špecifickými operáciami a cvičeniami, pri ktorých bola účasť krajín, ktoré nie sú členmi NATO, na túto činnosť schválené na základe individuálneho schválenia NAC, a

(iii) bezpečnostný orgán ACO (SHAPE J2) zavedie autoritatívny a kontrolovateľný proces uvoľňovania utajovaných skutočností ,

(d) veliteľ misie pre operáciu zahŕňajúcu krajiny, ktoré nie sú členmi a poskytujú svoj kontingent vojsk (NNTCN),
podľa schválenia NAC, pri informáciách so stupňom utajenia NS vrátane, ktoré už boli určené na uvoľnenie do misie (xFOR) za týchto podmienok:

(i) utajované skutočnosti sa týkajú konkrétnej misie,

(ii) utajované skutočnosti sú obmedzené na taktické informácie týkajúce sa prebiehajúcej operácie a považované za potrebné na úspešné vykonanie prebiehajúcej operácie,

(iii) bezpečnostný orgán misie zavedie autoritatívny a kontrolovateľný proces uvoľňovania utajovaných skutočností, a

(iv) NOS si v úzkej koordinácii so SHAPE J2 vyhradzuje právo vykonať kontroly bezpečnostných opatrení, ktoré sú v platnosti, a

(e) NPLO (Organizácia NATO pre výrobu a logistiku), pre utajované skutočnosti NATO, ktorých pôvodcom je jedna alebo viac krajín zúčastnených v NPLO.

38. Právomoc na uvoľnenie sa môže vecne delegovať len na príslušný výbor, v ktorom je pôvodca (-ovia) zastúpený/í. Ak pôvodcu(-ov) nemožno určiť, vecne príslušný výbor preberá zodpovednosť pôvodcu. Právomoc na vydanie môže byť delegovaná na najnižšiu úroveň výborov, ktorá je najvhodnejšia na vyhodnotenie dôležitosti utajovaných skutočností.

39. S výnimkou vzťahujúcou sa na utajované skutočnosti NR uvedené v odseku 37 písm. a) a b) hore, autority, na ktoré bola táto právomoc delegovaná už ďalej nemôžu delegovať svoju právomoc aj napriek tomu, že môžu poveriť nižšie orgány implementáciou rozhodnutia o uvoľnení.

40. Civilné a vojenské orgány NATO vedú kontrolné záznamy o utajovaných skutočnostiach so stupňom utajenia CONFIDENTIAL a vyšším, ktoré uvoľnili príjemcom mimo členských krajín NATO. Tieto záznamy podliehajú kontrole príslušného bezpečnostného orgánu NATO (napríklad NOS, SHAPE J2).

Administratívne opatrenia pre implementáciu bezpečnostnej dohody

41. Ukončenie administratívnych opatrení príslušných agentúr príjemcu z nečlenskej krajiny NATO, sa potvrdí bezpečnostnou previerkou, ktorú vykoná NOS. Bezpečnostná previerka potvrdí schopnosť príjemcu z nečlenskej krajiny NATO, spĺňať ustanovenia bezpečnostnej dohody a minimálnych štandardov.

42. NOS vypracuje správu z previerky a jej kópiu odošle bezpečnostnému úradu príjemcu z nečlenskej krajiny NATO. Originál správy sa uchová v NOS a na požiadanie sa sprístupní členským krajinám NATO. Bezpečnostný výbor NATO poskytne písomný súhrn výsledkov previerok NOS. Záver odvodený z tohto súhrnu poskytne NOS príslušným orgánom NATO a členským krajinám NATO, ako spôsobilosť príjemcu z nečlenskej krajiny NATO ochraňovať utajované skutočnosti NATO.

43. NOS vykonáva pravidelné bezpečnostné previerky, najmenej raz za dva roky, príslušných agentúr príjemcov z nečlenských krajín NATO pre zabezpečenie, aby príjemca, ktorý je z nečlenskej krajiny NATO, dodržiaval ustanovenia bezpečnostnej dohody a minimálne štandardy.

44. Ak sa NATO poskytne bezpečnostná záruka ohľadne ochrany uvoľnených utajovaných skutočností, zabezpečí sa každoročné potvrdenie jej platnosti, spolu s prehodnotením potreby prijímať takéto utajované skutočnosti. NOS taktiež zhodnotí, či by nebolo vhodnejšie vyjednať bezpečnostnú dohodu namiesto bezpečnostnej záruky. NOS vedie záznamy o potvrdeniach platnosti bezpečnostných záruk, ktoré tiež obsahujú dôvody k takýmto opätovným potvrdenia platnosti. Členským krajinám NATO sa na požiadanie poskytne kópia týchto záznamov.

Podporná smernica k administratívnej bezpečnosti

45. Podporná smernica k administratívnej bezpečnosti okrem iného obsahuje:

(a) postupy na uvoľňovanie utajovaných skutočností NATO príjemcom z nečlenských krajín NATO,

(b) osobitné postupy na uvoľňovanie pre organizáciu NATO pre výrobu a logistiku (NPLOs), medzinárodné organizácie a kombinované spoločné sily zvláštneho určenia (CJTFs),

(c) minimálne zásady potrebné pri manipulácii a ochrane utajovaných skutočností NATO uvoľnených príjemcom z nečlenskej krajiny NATO. Minimálne zásady sa vzťahujú na akéhokoľvek príjemcu z nečlenskej krajiny NATO, bez ohľadu na to, či bola uzavretá bezpečnostná dohoda s NATO alebo či bola poskytnutá bezpečnostná záruka NATO,

(d) podrobné administratívne opatrenia, ktoré majú implementovať všetci príjemcovia z nečlenských krajín NATO, a

(e) vzory bezpečnostných záruk, osvedčenie o vykonaní bezpečnostnej previerky a osvedčenie o bezpečnostnej previerke.

PRÍLOHA „F“

Bezpečnosť komunikačných a informačných systémov

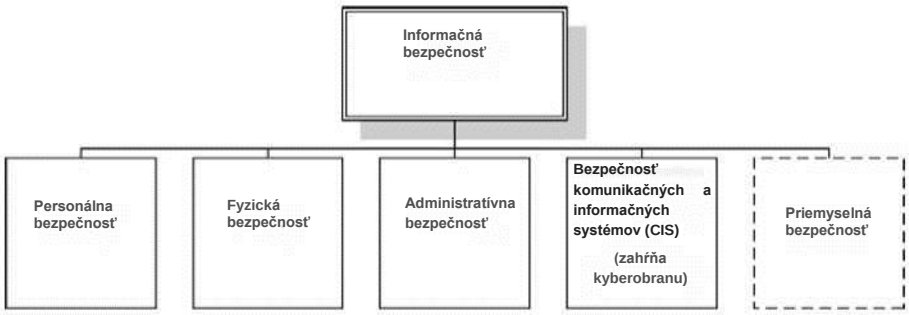
1. ÚVOD

1.1. Táto príloha stanovuje zásady a minimálne štandardy na ochranu utajovaných skutočností NATO a podporných systémových služieb a zdrojov[1] v komunikačných, informačných a iných elektronických systémoch, ktoré uchovávajú, spracovávajú alebo prenášajú utajované skutočnosti NATO.

1.2. Táto príloha podporuje Politiku riadenia utajovaných skutočností NATO (NIMP) a dopĺňa Politiku riadenia neutajovaných informácií NATO, ktorá sa zaoberá základnými zásadami a normami, ktoré sa majú uplatňovať v rámci civilných a vojenských orgánov NATO a členských krajín NATO na ochranu neutajovaných informácií NATO.

1.3. Bezpečnosť komunikačných a informačných systémov (bezpečnosť CIS) je jedným z prvkov systému Informačnej bezpečnosti (obr. 1) a je definovaná ako uplatňovanie bezpečnostných opatrení na ochranu komunikačných, informačných a iných elektronických systémov[1] [2] a informácií, ktoré sú v týchto systémoch[3] ukladané, spracovávané alebo prenášané s ohľadom na dôvernosť, integritu, dostupnosť, autentifikáciu a nespochybniteľnosť.

1.4. Aby sa dosiahli bezpečnostné ciele dôvernosti, integrity, dostupnosti, autentifikácie a nespochybniteľnosti[4] pre utajované skutočnosti spracované v týchto CIS, zavedie sa vyvážený súbor bezpečnostných opatrení (fyzické, personálne, informačné a CIS), aby sa vytvorilo bezpečné prostredie, v ktorom sa bude prevádzkovať CIS. Pri spracovaní utajovaných informácií v priemysle pri zmluvách sa uplatňujú ďalšie osobitné opatrenia priemyselnej bezpečnosti v súlade s prílohou G tohto CM dokumentu a podpornou smernicou o priemyselnej bezpečnosti.



Obrázok 1 - Vzťah medzi zabezpečením informácií a bezpečnosťou CIS

[1] Služby a zdroje podporných systémov - tie služby a zdroje potrebné na zabezpečenie dosiahnutia bezpečnostných cieľov CIS; zahrnúť napríklad šifrové produkty a mechanizmy, materiály COMSEC, telefónne zoznamy a environmentálne zariadenia a kontroly.

[2] Ďalej uvedené v tejto prílohe ako CIS.

[3] Ďalej uvedené v tejto prílohe ako „ s ktorými sa manipuluje“.

[4] Ďalej uvedené v tejto prílohe ako bezpečnostné ciele.

1.5. „Primárna smernica o bezpečnosti CIS“, ktorú vydáva SC a C3B na podporu tejto politiky rieši činnosti Bezpečnosti CIS počas životného cyklu CIS a zodpovednosti Bezpečnosti CIS výborov, a civilných a vojenských orgánov NATO. „Primárna smernica o bezpečnosti CIS“ je podporená smernicami, ktoré sa zaoberajú riadením Bezpečnosti CIS (vrátane riadenia bezpečnostných rizík, bezpečnostnej akreditácie, dokumentácie súvisiacej s bezpečnosťou a preskúmaním/kontrolou bezpečnosti) a technických a implementačných aspektov zabezpečenia CIS (vrátane počítačovej a lokálnej siete (LAN), prepojenia zabezpečenia sietí, šifrovej bezpečnosti, bezpečnosti prenosu a bezpečnosti vysielania).

2. BEZPEČNOSTNÉ CIELE

2.1. Na dosiahnutie primeranej bezpečnostnej ochrany utajovaných skutočností NATO, s ktorými sa manipuluje v CIS, sa odsúhlasí a zavedie vyvážený súbor bezpečnostných opatrení (fyzických, personálnych, informačných a CIS) s cieľom vytvoriť bezpečné prostredie, v ktorom funguje CIS tak, aby sa splnili nasledujúce bezpečnostné ciele:

(a) zabezpečiť dôvernosť informácií kontrolovaním zverejňovania a prístupu k utajovaným skutočnostiam NATO a podporou systémových služieb a zdrojov,

(b) zabezpečiť integritu utajovaných skutočností NATO a podporovať systémové služby a zdroje,

(c) zabezpečiť dostupnosť utajovaných skutočností NATO a podporovať systémové služby a zdroje,

(d) zabezpečiť spoľahlivú identifikáciu a autentifikáciu osôb, zariadení a služieb, ktoré pristupujú k CIS spracúvajúcim utajované skutočnosti NATO, a

(e) zabezpečiť primeranú nespochybniteľnosť pre osoby a subjekty, ktoré spracovali utajované skutočnosti.

2.2. Utajované skutočnosti NATO a podporné systémové služby a zdroje musia byť chránené minimálnym súborom opatrení zameraných na zabezpečenie všeobecnej ochrany pred bežnými problémami (či už náhodnými alebo úmyselnými), o ktorých je známe, že postihujú všetky systémy a podporné systémové služby a zdroje. Musia sa prijať dodatočné opatrenia primerané okolnostiam, keď posúdenie bezpečnostného rizika preukázalo, že utajované skutočnosti NATO a/alebo podporné systémové služby a zdroje podliehajú zvýšenému riziku v dôsledku špecifických hrozieb a zraniteľných miest.

2.3. Nezávisle od bezpečnostného stupňa utajenia utajovaných skutočností NATO, s ktorými sa manipuluje, bezpečnostné orgány NATO vyhodnotia riziká a úroveň škôd, ktoré vzniknú NATO, ak zlyhajú opatrenia na dosiahnutie bezpečnostných cieľov, ktoré nemajú dôverný charakter.
Minimálny súbor opatrení týkajúcich sa služieb, ktoré nemajú dôverný charakter, sa určí v súlade so smernicami podporujúcimi túto politiku.

3. BEZPEČNOSTNÁ CERTIFIKÁCIA

3.1. Rozsah, v ktorom sa majú splniť bezpečnostné ciele, a rozsah, v akom je potrebné sa spoliehať na bezpečnostné opatrenia CIS na zabezpečenie utajovaných skutočností NATO a podporných systémových služieb a zdrojov, budú určené v procese zavedenia bezpečnostnej požiadavky.
Proces bezpečnostnej certifikácie stanoví, že sa dosiahla primeraná úroveň ochrany a dodržiava sa.

3.2. Všetky CIS, v ktorých sa manipuluje s utajovanými skutočnosťami NATO podliehajú procesu bezpečnostnej certifikácie, ktorý rieši bezpečnostné ciele.

4. PERSONÁLNA BEZPEČNOSŤ

4.1. Osoby oprávnené na prístup k utajovaným skutočnostiam NATO v akejkoľvek forme musia byť bezpečnostne preverené na primeraný stupeň, berúc do úvahy ich celkové povinnosti , ak je to vhodné, pri zohľadnení ich celkovej zodpovednosti za dosiahnutie bezpečnostných cieľov informácií a podporných systémových služieb a zdrojov. To zahŕňa osoby s oprávnením na prístup k podporným systémovým službám a zdrojom alebo ktoré sú zodpovedné za ich ochranu, i keď tieto nie sú oprávnené na prístup k utajovaným skutočnostiam, s ktorými sa manipuluje v rámci systému.

5. FYZICKÁ BEZPEČNOSŤ

5.1. Priestory, v ktorých sa utajované skutočnosti NATO prezentujú alebo sa s nimi manipuluje s použitím informačných technológií alebo kde je možný prístup k takýmto utajovaným skutočnostiam, sa zabezpečia tak, aby bola splnená súhrnná požiadavka na bezpečnostné ciele.

6. ADMINISTRATÍVNA BEZPEČNOSŤ

6.1. Všetky utajované počítačové pamäťové médiá musia byť riadne označené, uložené a chránené takým spôsobom, ktorý zodpovedá najvyššiemu stupňu utajenia utajovaných skutočností uložených na médiu.

6.2. Utajované skutočnosti NATO, zaznamenané na opakovane použiteľných počítačových pamäťových médiách, sa vymažú iba v súlade s postupmi schválenými príslušným bezpečnostným orgánom.

6.3. Schválené bezpečnostné opatrenia (dôvernosť a otvorenosť) zavedené v súlade so smernicami na podporu tejto politiky, sa môžu použiť na ochranu utajovaných skutočností NATO, uložených na počítačových pamäťových médiách takým spôsobom, že sa zredukujú požiadavky na fyzickú bezpečnosť zodpovedajúce nižšiemu stupňu utajenia.

7. PRIEMYSELNÁ BEZPEČNOSŤ

7.1. Priestory dodávateľa použité na kontrakty, v ktorých sa manipuluje s utajovanými skutočnosťami NATO v CIS, sa zariadia tak, aby spĺňali celkové požiadavky na bezpečnostné ciele.

7.2. V kontraktoch, listoch o bezpečnostnej stránke (SAL) a/alebo v bezpečnostných inštrukciách projektu (PSI) a/alebo v dohodách na úrovni služby (SLA), podľa aplikovateľnosti, sa popíše celkový súbor opatrení CIS, ktoré dodávatelia implementujú s cieľom plniť bezpečnostné ciele CIS NATO a chrániť utajované skutočnosti NATO a podporné služby.

8. BEZPEČNOSTNÉ OPATRENIA

8.1. Na všetky CIS, v ktorých sa manipuluje s utajovanými skutočnosťami NATO, sa aplikuje dôsledný súbor bezpečnostných opatrení s cieľom splniť bezpečnostné ciele na ochranu utajovaných skutočností a podporných systémových služieb a zdrojov. Bezpečnostné opatrenia zahŕňajú v prípade potreby nasledujúce:

(a) prostriedky, ktoré poskytnú dostatočné informácie na zabezpečenie prešetrenia úmyselného, náhodného vyzradenia alebo pokusu o vyzradenie bezpečnostných cieľov utajovaných skutočností a podporných systémových služieb a zdrojov, úmerné možným škodám, ktoré by boli spôsobené,

(b) spôsob spoľahlivej identifikácie a autentifikácie oprávnených prístupov osôb, zariadení a služieb. Informácie a materiál, ktoré kontrolujú prístup do systému CIS, sa kontrolujú a chránia podľa opatrení primeraných k informáciám, ku ktorým môžu dávať prístup. Na utajované skutočnosti CIS NATO sa musia zaviesť silné mechanizmy na autentifikáciu osôb,

(c) spôsob kontroly sprístupňovania a prístupu k utajovaným skutočnostiam NATO a k podporným systémovým službám a zdrojom založeným na základe princípu „need-to-know“,

(d) prostriedok na overenie integrity a pôvodu utajovaných skutočností NATO a podporných systémových služieb a zdrojov,

(e) prostriedok na zachovanie celistvosti utajovaných skutočností NATO a podporných systémových služieb a zdrojov,

(f) prostriedok na zachovanie dostupnosti utajovaných skutočností NATO a podporných systémových služieb a zdrojov,

(g) prostriedok na kontrolu spojenia CIS, ktorý spracúva utajované skutočnosti NATO,

(h) určenie dôvernosti, ktorá sa udelí ochranným mechanizmom bezpečnosti CIS,

(i) prostriedok na posúdenie a overenie riadneho fungovania mechanizmov ochrany bezpečnosti CIS počas životného cyklu CIS,

(j) prostriedok na prešetrenie používateľa a činnosti CIS,

(k) prostriedok na poskytnutie nespochybniteľných záruk, že odosielateľovi informácie bude poskytnutý doklad o doručení a príjemcovi bude poskytnutý dôkaz o totožnosti odosielateľa, a

(l) prostriedok na ochranu ukladaných utajovaných skutočností NATO v prípade, že opatrenia fyzickej bezpečnosti nespĺňajú minimálne štandardy.

8.2. Na zabránenie, prevenciu, zisťovanie a odolávanie a obnovu z dôsledkov aktivít postihujúcich bezpečnostné ciele utajovaných skutočností NATO a podporných systémových služieb a zdrojov, vrátane hlásenia bezpečnostných incidentov

8.3. Bezpečnostné opatrenia sa riadia a implementujú v súlade so smernicami podporujúcimi túto politiku.

9. RIADENIE BEZPEČNOSTNÝCH RIZÍK

9.1. CIS, v ktorých sa manipuluje s utajovanými skutočnosťami NATO v civilných a vojenských orgánoch NATO podliehajú riadeniu bezpečnostných rizík , vrátane hodnotenia bezpečnostného rizika, v súlade so smernicami podporujúcich túto politiku.

9.2. Riadenie bezpečnostného rizika v systéme CIS NATO musí zabezpečiť nepretržité vyhodnocovanie zraniteľnosti systému a dodržiavanie bezpečnostných požiadaviek a smerovanie k dynamickému riadeniu rizík, aby bolo schopné účinne čeliť výzvam, ktoré predstavujú súčasné komplexné operačné scenáre a mnohostranné rizikové prostredia.

10. ELEKTROMAGNETICKÝ PRENOS [5] UTAJOVANÝCH SKUTOČNOSTÍ NATO

10.1. Keď sa utajované skutočnosti NATO prenášajú elektromagneticky, musia byť prijaté osobitné opatrenia na dosiahnutie bezpečnostných cieľov takýchto prenosov. Orgány NATO určia požiadavky na ochranu prenosov pred detekciou, odpočúvaním alebo zneužívaním.

11. ŠIFROVÁ BEZPEČNOSŤ:

11.1. Ak sa na zabezpečenie ochrany dôvernosti a otvorenosti, či už počas prenosu, spracovania alebo ukladania informácií (uložené údaje) vyžadujú šifrové produkty alebo mechanizmy, musia byť takéto produkty alebo mechanizmy osobitne schválené na tento účel a musia byť zavedené špecifické šifrovacie požiadavky na fyzické, procesné a technické opatrenia na dosiahnutie požadovaných bezpečnostných cieľov.

11.2. Uložené údaje musia byť chránené na úrovni primeranej k požadovaným bezpečnostným cieľom a ak sa používajú šifrové produkty a mechanizmy, požiadavky na šifrovaciu bezpečnosť musia byť v súlade s príslušnými technickými a vykonávacími smernicami NATO.

11.3. Počas prenosu je dôvernosť utajených skutočností so stupňom utajenia NS a vyšším chránená šifrovými produktmi alebo mechanizmami schválenými Vojenským výborom NATO (NAMILCOM).

11.4. Počas prenosu je dôvernosť utajovaných skutočností so stupňom utajenia NC alebo NR chránená šifrovými produktmi alebo mechanizmami schválenými buď zo strany NAMILCOM alebo členskou krajinou NATO.

11.5. Počas prenosu musia byť požiadavky na otvorenosť zabezpečené v súlade s prevádzkovými požiadavkami komunikačného systému. Hodnotiace požiadavky a schvaľovací orgán pre mechanizmy otvorenosti založené na šifrovaní musia byť identifikované a odsúhlasené v spojení so špecifikáciou takýchto mechanizmov v prevádzkových požiadavkách, podľa dohody v technických smerniciach.

[5.] Pojem „elektromagnetický prenos“ zahŕňa prenos, ktorý má elektrický a magnetický charakter alebo vlastnosti a okrem iného zahŕňa viditeľné svetlo, rádiové vlny, mikrovlnné žiarenie a infračervené žiarenie.

11.6. Za výnimočných prevádzkových okolností môžu byť utajované skutočnosti so stupňom utajenia NC a NS zasielané v otvorenej forme za predpokladu, že každá okolnosť bude riadne ohlásená vyšším orgánom. Výnimočné okolnosti sú nasledovné:

(a) počas hroziacej alebo skutočnej krízy, konfliktov alebo vojnových situácií, a

(b) ak je rýchlosť doručenia mimoriadne dôležitá, prostriedky šifrovania nie sú k dispozícii a odhaduje sa, že prenášané utajované skutočnosti nemožno zneužiť v čase, na nepriaznivé ovplyvnenie operácií.

11.7. Za výnimočných okolností, ak je rýchlosť doručenia mimoriadne dôležitá, prostriedky šifrovania nie sú k dispozícii a odhaduje sa, že prenášané utajované skutočnosti nemožno zneužiť v čase, na nepriaznivé ovplyvnenie operácií, utajované skutočnosti so stupňom utajenia NR môžu byť prenášané v otvorenej forme.

11.8. Počas prenosu medzi CIS NATO a nečlenských krajín NATO/medzinárodných organizácií (NNN/IO) bude dôvernosť utajovaných skutočností so stupňom utajenia NS a vyšším chránená šifrovými produktmi alebo mechanizmami schválenými Vojenským výborom NATO (NAMILCOM).

11.9. Počas prenosu v rámci CIS nečlenských krajín NATO/medzinárodných organizácií (NNN/IO) musí byť dôvernosť utajovaných skutočností so stupňom utajenia NS a vyšším, chránená šifrovými produktami alebo mechanizmami schválenými Vojenským výborom NATO (NAMILCOM).

11.10. Ak nie je možné splniť požiadavky uvedené v bodoch 11.8 a 11.9 vyššie, NATO a medzinárodná organizácia môžu dosiahnuť dohodu o vzájomnom uznávaní postupov hodnotenia, výberu a schvaľovania šifrových produktov alebo mechanizmov schválených na ochranu pri prenose utajovaných skutočností NS alebo utajovaných skutočností medzinárodnej organizácie s rovnocenným stupňom utajenia. Podmienky takéhoto prijatia sú uvedené v bode 11.12.

11.11. Za výnimočných okolností môže NATO s cieľom podporiť špecifické prevádzkové požiadavky, a keď nemožno splniť požiadavky bodov 11.8 a 11.9 vyššie, odsúhlasiť procesy hodnotenia, výberu a schvaľovania nečlenských štátov NATO pre šifrové produkty alebo mechanizmy schválené na ochranu prenosu utajovaných skutočností NS alebo utajovaných skutočností nečlenských krajín NATO s rovnocenným stupňom utajenia. Podmienky takejto dohody sú uvedené v odseku 11.12 nižšie.

11.12. Pre scenáre uvedené v bodoch 11.10 a 11.11 vyššie sa uplatňujú tieto podmienky:

a) nečlenská krajina NATO/medzinárodná organizácia musí mať uzatvorenú bezpečnostnú dohodu s NATO a musí byť certifikovaná Bezpečnostným úradom NATO (NOS), že dokáže primerane chrániť utajované skutočnosti uvoľnené zo strany NATO,

b) každá nečlenská krajina NATO/medzinárodná organizácia sa bude posudzovať od prípadu k prípadu, a základ akéhokoľvek súhlasu bude stanovený v bezpečnostných opatreniach podporujúcich bezpečnostnú dohodu medzi NATO a nečlenskou krajinou NATO/medzinárodnou organizáciou,

(c) podmienky akéhokoľvek takéhoto súhlasu musí schváliť NAMILCOM na základe objektívneho hodnotenia vykonaného NOS v spolupráci Agentúrou NAMILCOM pre bezpečnosť a hodnotenie komunikačných a informačných systémov (SECAN), Výborom C3B a schopnosti kybernetickej obrany a personálom NATO HQ C3, schopnosti nečlenskej krajiny NATO/medzinárodnej organizácie vykonávať šifrovacie hodnotenia, ktoré spĺňajú požiadavky ekvivalentné požiadavkám používaným v rámci NATO na šifrovú ochranu utajovaných skutočností NS, a

(d) NOS v spolupráci so SECAN a personálom NATO HQ C3 sa prostredníctvom overovania a pravidelného opätovného overovania ubezpečia, že členská krajina/medzinárodná organizácia má zavedené vhodné štruktúry, pravidlá a postupy na hodnotenie, výber, schválenie a kontrolu šifrovacích produktov a mechanizmov a že tieto štruktúry, pravidlá a postupy sa účinne a bezpečne uplatňujú v praxi.

11.13. Ak sa dosiahne prijatie/dohoda v súlade s podmienkami stanovenými v bode 11.12 vyššie, dôvernosť informácií klasifikovaných ako NS môže byť chránená buď šifrovými produktmi alebo mechanizmami schválenými Vojenským výborom NATO (NAMILCOM), alebo šifrovacími produktmi alebo mechanizmami schválenými NCSA (alebo rovnocenným orgánom) nečlenskej krajiny NATO/medzinárodnej organizácie pre ochranu ekvivalentného stupňa utajenia.

11.14. Počas prenosu medzi NATO a CIS nečlenskej krajiny NATO/medzinárodnej organizácie a v rámci CIS nečlenskej krajiny NATO/medzinárodnej organizácie bude dôvernosť utajovaných skutočností so stupňom utajenia NS a vyšším chránená šifrovanými produktmi alebo mechanizmami vyhodnotenými a schválenými príslušným orgánom. Príslušný orgán môže byť NAMILCOM, NCSA členskej krajiny NATO alebo ekvivalentný orgán nečlenskej krajiny NATO/medzinárodnej organizácie za predpokladu, že nečlenská krajina NATO/medzinárodná organizácia má zavedené vhodné štruktúry, pravidlá a postupy na hodnotenie, výber, schválenie a kontrolu šifrových produktov a mechanizmov a že tieto štruktúry, pravidlá a postupy sa účinne a bezpečne uplatňujú v praxi. Štruktúry, pravidlá a postupy sa dohodnú medzi NAMILCOM a nečlenskou krajinou NATO/medzinárodnou organizáciou.

11.15. Citlivosť šifrového materiálu použitého na ochranu utajovaných skutočností NATO si vyžaduje uplatnenie osobitných bezpečnostných opatrení, okrem tých, ktoré sú potrebné na ochranu ostatných utajovaných skutočností NATO.

11.16. Ochrana, ktorá bude poskytnutá šifrovému materiálu, musí zodpovedať poškodeniu, ktoré môže vzniknúť, ak ochrana zlyhá. Musia existovať pozitívne prostriedky na posúdenie a overenie ochrany a riadneho fungovania šifrových produktov a mechanizmov a ochranu a kontrolu šifrových utajovaných skutočností (napr. podrobnosti o implementácii a súvisiaca dokumentácia).

11.17. Vzhľadom na mimoriadnu citlivosť šifrovaných utajovaných skutočností existujú v rámci NATO a v rámci každej členskej krajiny osobitné predpisy a orgány, ktoré riadia prijatie, kontrolu a šírenie šifrovaných utajovaných skutočností NATO pre osoby so špeciálnym oprávnením.

11.18. Musia byť tiež dodržané osobitné postupy, ktoré regulujú výmenu technických utajovaných skutočností a ktoré regulujú výber, výrobu a obstarávanie šifrových produktov a mechanizmov.

12. BEZPEČNOSŤ NEŽIADÚCEHO ELEKTROMAGNETICKÉHO VYŽAROVANIA

12.1. Na ochranu pred zneužitím utajovaných skutočností so stupňom utajenia NC a vyšším prostredníctvom nežiaduceho elektromagnetického vyžarovania, sa zavedú bezpečnostné opatrenia. Tieto opatrenia zodpovedajú stupňu zneužitia a citlivosti utajovaných skutočností.

13. ŠPECIFICKÉ ZODPOVEDNOSTI BEZPEČNOSTI CIS

13.1. Vojenský výbor NATO (NAMILCOM)

13.1.1. Medzi zodpovednosti NAMILCOM za oblasť bezpečnosti CIS patrí bezpečnostné schvaľovanie šifrových prostriedkov a účasť na hodnotení a výbere šifrových produktov a mechanizmov pre štandardné používanie NATO. Štyri agentúry pozostávajúce z predstaviteľov členských krajín Vojenského výboru (SECAN, DACAN, EUSEC a EUDAC) poskytujú poradenstvo a podporu pre bezpečnosť CIS pre NAMILCOM, SC, C3B a podľa potreby pre ich podštruktúry členským krajinám a ostatným organizáciám NATO.

13.2. Výbor C3Board (C3B)

13.2.1. Ako najvyšší výbor pre politiku v oblasti poradenstva, velenia a kontroly (C3) v rámci Aliancie C3B podporuje NAMILCOM a politické orgány NATO v ich procese overovania kapacít a projektov C3 na základe preskúmania prevádzkových požiadaviek C3. C3B je zodpovedný za poskytovanie bezpečných a interoperabilných systémov C3 v celom NATO. Podporný personál pre C3B sa poskytuje z NATO HQ C3 (NHQC3S).

13.3. Rada NATO pre riadenie kybernetickej obrany (CDMB)

13.3.1 CDMB je koordinačný orgán pre kybernetickú obranu, ktorý poskytuje strategické plánovanie a smerovanie implementácie politiky kybernetickej obrany a uľahčuje spoluprácu so spojencami. CDMB podáva hlásenia a získava politické usmernenia od NAC prostredníctvom Výboru pre obrannú politiku a plánovanie v zosilnenom formáte (DPPC(R)). CDMB je pod dohľadom spojencov prostredníctvom C3B v oblasti politiky C3 a implementačných aspektoch kybernetickej obrany. CDMB konzultuje o konkrétnych záležitostiach prostredníctvom príslušných výborov NATO.

13.4. Národný úrad pre bezpečnosť CIS (NCSA)

13.4.1. Každá členská krajina NATO aj krajina, ktorá nie je členom NATO, ak je to vhodné, ustanoví NCSA, ktorý môže byť zriadený ako agentúra v národnej bezpečnostnej infraštruktúre. NCSA je zodpovedný za:

(a) kontrolu šifrových technických utajovaných skutočností týkajúcich sa ochrany utajovaných skutočností NATO v rámci danej krajiny,

(b) zabezpečenie, aby boli šifrové systémy, produkty a mechanizmy na ochranu utajovaných skutočností NATO náležite vybrané, prevádzkované a udržiavané,

(c) zabezpečenie, aby boli bezpečnostné produkty CIS na ochranu utajovaných skutočností NATO primerane vybraté, prevádzkované a udržiavané v rámci svojej krajiny,

(d) komunikáciu o bezpečnostných a technických otázkach bezpečnosti civilného a vojenského systému CIS s príslušnými orgánmi NATO a orgánmi krajiny, a

(e) identifikáciu národného orgánu TEMPEST podľa potreby.

13.4.2. NCSA spolupracujú v koordinácii so svojimi národnými bezpečnostnými úradmi (NSA).

13.5. **Národný distribučný orgán (NDA)**

13.5.1. Každá členská a, ak je to relevantné, aj nečlenská krajina NATO určí NDA, ktorý môže byť zriadený ako agentúra v národnej bezpečnostnej infraštruktúre, ktorá je zodpovedná za správu šifrového materiálu NATO v rámci svojej krajiny, a zabezpečuje, aby boli zavedené a uplatňované kanály pre komplexné účtovanie, bezpečnú manipuláciu, uchovávanie, distribúciu a zničenie všetkého šifrového materiálu.

13.5.2. NDA spolupracujú v koordinácii so svojimi národnými bezpečnostnými úradmi (NSA).

13.6. **Orgán (-y) pre bezpečnostnú certifikáciu**

13.6.1. Každý členská a, ak je to relevantné, aj nečlenská krajina NATO, si určí svoju bezpečnostnú schvaľovaciu alebo akreditačnú autoritu (-y), ktorá zodpovedá za bezpečnostné schvaľovanie alebo akreditáciu nasledovných orgánov:

a) národných komunikačných a informačných systémov CIS, prostredníctvom ktorých sa manipuluje s utajovanými skutočnosťami NATO, a

b) CIS NATO, ktoré sú v prevádzke v rámci národných orgánov alebo organizácií.

13.6.2. Ak je v rámci členskej krajiny NATO založený civilný alebo vojenský orgán NATO, CIS NATO bude predmetom bezpečnostnej certifikácie zo strany bezpečnostného akreditačného úradu (NATO SAA). V takomto prípade môže byť bezpečnostná akreditácia koordinovaná s príslušným vnútroštátnym bezpečnostným certifikačným orgánom.

13.7. **Bezpečnostný certifikačný orgán NATO (SAA)**

13.7.1. Existujú tri NATO SAA zodpovedné za bezpečnostnú certifikáciu CIS NATO, v ktorých sa manipuluje s utajovanými skutočnosťami NATO. SAA je riaditeľ, Bezpečnostný úrad NATO alebo strategický veliteľ, alebo ich delegovaní / nominovaní zástupcovia v závislosti od CIS, ktorý sa má certifikovať.

13.7.2. Bezpečnostná certifikačná rada CIS NATO zložená z NATO SAA identifikovaného podľa predchádzajúceho odseku, má bezpečnostný certifikačný dohľad nad všetkými CIS NATO, v ktorých sa manipuluje s utajovanými skutočnosťami NATO tak, aby zabezpečila jednotný a konzistentný prístup k bezpečnosti CIS NATO. Podmienky Bezpečnostnej certifikačnej rady CIS NATO podliehajú schvaľovaniu v Bezpečnostnom výbore (SC).

13.8. **Bezpečnostný orgán pre nečlenskú krajinu NATO (NNN)**

13.8.1. Nečlenská krajina NATO (NNN) vymenuje bezpečnostný orgán, ktorý bude zodpovedný za bezpečnostné opatrenia tejto prílohy a dohľad nad orgánmi nečlenskej krajiny NATO so špecifickými zodpovednosťami v oblasti bezpečnosti CIS za národné CIS, v ktorých sa manipuluje s utajovanými skutočnosťami v rámci CIS (vrátane NCSA, NDA a SAA).

PRÍLOHA „G“

UTAJOVANÝ PROJEKT A PRIEMYSELNÁ BEZPEČNOSŤ

ÚVOD

1. Táto príloha sa zaoberá bezpečnostnými aspektmi priemyselných operácií, ktoré sú jedinečné pri rokovaniach a uzatváraní zmlúv, ktoré obsahujú utajované skutočnosti NATO a ich plnenie zo strany priemyslu vrátane uvoľnenia utajovaných skutočností NATO počas predzmluvných rokovaní a plnenia zmluvy. Táto príloha stanovuje bezpečnostnú politiku pre:

(a) bezpečnostné požiadavky na predkladanie ponúk, prerokovanie a uzatváranie zmlúv obsahujúcich utajované skutočnosti NATO,

(b) zmluvy obsahujúce utajované skutočnosti NATO s dodávateľmi v nečlenských krajinách NATO,

(c) potvrdenie o priemyselnej bezpečnosti týkajúce sa zmlúv, ktoré zahŕňajú utajované skutočnosti NATO (previerka priemyselnej bezpečnosti (FSC) a bezpečnostné previerky osôb (PSC)),

(d) uvoľnenie utajovaných skutočností NATO pri uzatváraní zmlúv,

(e) spracovanie utajovaných skutočností NATO v komunikačných a informačných systémoch (CIS),

(f) postupy kontroly medzinárodných návštev (IVCP), a

(g) medzinárodný prenos a preprava utajovaného materiálu NATO,

2. Táto príloha sa opiera o smernicu o utajovaných projektoch a priemyselnej bezpečnosti, ktorá stanovuje podrobné požiadavky a postupy.

SÚŤAŽENIE, ROKOVANIA A UZATVÁRANIE ZMLÚV SÚVISIACICH S UTAJOVANÝMI INFORMÁCIAMI NATO

3. Hlavná zmluva o programe/projekte NATO bude prerokovaná a uzatvorená agentúrou/úradom pre programy/projekty NATO (NPA/NPO). FSC sa bude vyžadovať od všetkých zmluvných partnerov zapojených do zmlúv, ktoré vyžadujú, aby poskytovateľ mohol spracúvať, generovať alebo mať prístup k utajovaným skutočnostiam NATO so stupňom utajenia CONFIDENTIAL (NC) a vyšším. V prípade zmlúv so stupňom utajenia NATO RESTRICTED (NR) sa nevyžaduje FSC.

4. NPA/NPO alebo iný verejný obstarávateľ, ktorý iniciuje zmluvu, zabezpečí, aby zariadenia dodávateľa mali príslušnú FSC pre konkrétnu fázu zmluvy. Verejný obstarávateľ overí, či personál dodávateľa, ktorý pristupuje k utajovaným skutočnostiam so stupňom utajenia NC alebo vyšším v priestoroch verejného obstarávateľa, má príslušné PSC.

5. Po prevzatí hlavnej zmluvy môže hlavný dodávateľ rokovať o subdodávkach s inými dodávateľmi, t.j. subdodávateľmi. Títo subdodávatelia môžu tiež dojednať subdodávky s inými subdodávateľmi. Ak tieto subdodávky vyžadujú prístup k utajovaným skutočnostiam so stupňom utajenia NC a vyšším, uplatňujú sa požiadavky na priemyselnú a personálnu bezpečnosť uvedené v časti „Bezpečnostné previerky na priemyselné účely pre zmluvy NATO“ tejto prílohy a v smernici o utajených projektoch a priemyselnej bezpečnosti. Ak sa potenciálny subdodávateľ nachádza pod jurisdikciou[1] nečlenskej krajiny NATO, musí byť získané *predchádzajúce* povolenie na rokovanie o subdodávke od NPA/NPO alebo iného verejného obstarávateľa. Ak NPA/NPO uložila obmedzenia na uzatvárania zmlúv s krajinami NATO, ktoré nie sú účastníkmi programu alebo projektu, NPA/NPO bude vyzvaná, aby zvážila a udelila povolenie pred zmluvnými rokovaniami s dodávateľmi z týchto krajín.

6. Po pridelení hlavného kontraktu NPA/NPO alebo iný verejný obstarávateľ informuje NSA/DSA o hlavnom dodávateľovi a zabezpečí, aby list o bezpečnostnej stránke (SAL) a /alebo bezpečnostné inštrukcie k projektu (PSI) boli, ak je to možné poskytnuté hlavnému dodávateľovi spolu s kontraktom.

BEZPEČNOSTNÉ POŽIADAVKY NA UTAJOVANÉ KONTRAKTY NATO

7. Hlavný dodávateľ a subdodávatelia sú zmluvne povinní pod hrozbou ukončenia ich zmluvy prijať všetky opatrenia predpísané zo strany NSA/DSA na ochranu všetkých utajovaných skutočností NATO vytvorených dodávateľom alebo zverených dodávateľovi alebo obsiahnutých v položkách vyrábaných dodávateľom.

(a) Zmluvy na hlavný program/projekty zahŕňajúce utajované skutočnosti NATO budú obsahovať PSI ako prílohu; „Príručka k bezpečnostnému utajeniu projektu“ bude tvoriť súčasť PSI. Všetky ostatné zmluvy, ktoré obsahujú utajované skutočnosti NATO, musia zahŕňajú minimálne SAL, čo môže byť PSI, ktorého rozsah je obmedzený. V druhom prípade môže byť príručka pre bezpečnostné utajenia programu/projektu označovaná ako „kontrolný zoznam bezpečnostných stupňov utajenia“.

PSI dopĺňa bezpečnostné politiky a požiadavky NATO, zavádza osobitné bezpečnostné postupy spojené s príslušným programom/projektom NATO a prideľuje zodpovednosť za implementáciu bezpečnostných opatrení týkajúcich sa utajovaných skutočností.

(b) V prípade zmlúv týkajúcich sa len utajovaných skutočností NR boli v smernici o utajovaných projektoch a priemyselnej bezpečnosti stanovené osobitné predpisy, najmä v jej prílohe 4 „Zmluvná doložka o zabezpečení pre súťaženie a zmluvy obsahujúce utajované skutočnosti NATO RESTRICTED“.

8. Stupeň utajenia utajovaných skutočností prvkov programov/projektov, ktoré súvisia s možnými subdodávkami bude založený na Príručke k bezpečnostnému utajeniu projektu.

1 Právomoc nad predmetom alebo územím/zemepisnou oblasťou

ZMLUVY OBSAHUJÚCE UTAJOVANÉ SKUTOČNOSTI NATO S DODÁVATEĽMI V NEČLENSKÝCH KRAJINÁCH NATO

9. Uzatváranie zmlúv, ktoré obsahujú utajované skutočnosti NATO s dodávateľmi v nečlenských krajinách NATO, predstavuje uvoľnenie utajovaných skutočností a musí byť v súlade s prílohou E k C-M (2002)49, smernicou o administratívnej bezpečnosti a smernicou o utajovaných projektoch a priemyselnej bezpečnosti. Uvoľnenie bude vždy podliehať súhlasu príslušného pôvodcu(-ov).

10. Zmluvy obsahujúce utajované skutočnosti NATO s dodávateľmi v nečlenských krajinách NATO si vyžadujú existenciu dvojstrannej bezpečnostnej dohody medzi NATO alebo zmluvnou/ sponzorujúcou krajinou NATO a nečlenskou krajinou, kde je dodávateľ pod jurisdikciou NSA/DSA alebo iným kompetentným orgánom, ktorý má právomoc zaviazať dodávateľa na poskytnutie požadovanej ochrany. Ak sa zmluva riadi dvojstrannou bezpečnostnou dohodou medzi zmluvnou/ sponzorujúcou krajinou NATO a nečlenskou krajinou, krajina NATO poskytne NATO písomné potvrdenie, že poskytnuté utajované skutočnosti NATO sú upravené v rámci tejto bezpečnostnej dohody. Kópia potvrdenia sa poskytne BÚN a príslušnej NPO/NPA.

11. Uzatvorenie zmluvy s dodávateľom z nečlenskej krajiny NATO musí prebiehať podľa postupov stanovených v smernici o utajovaných projektoch a priemyselnej bezpečnosti.

12. Pre nečlenské krajiny NATO musí byť určený príslušný bezpečnostný orgán(-y), ktorý plní ekvivalentné funkcie ako NSA/DSA v členskej krajine NATO.

PREVIERKY PRIEMYSELNEJ BEZPEČNOSTI PRE KONTRAKTY

Všeobecné

13. Politika opísaná v nasledujúcich odsekoch pre subjekty a osoby je relevantná pre kontrakty a subkontrakty.

Bezpečnostné previerky subjektu (FSC)

14. NSA/DSA každej členskej krajiny NATO je zodpovedný za zabezpečenie toho, aby každý subjekt pod jeho jurisdikciou, ktorý bude vyžadovať prístup k utajovaným skutočnostiam so stupňom utajenia NC a vyšším, prijalo ochranné bezpečnostné opatrenia potrebné na získanie FSC. Pri udeľovaní FSC musí NSA/DSA zabezpečiť, aby mali prostriedky na to, aby boli poučení o všetkých okolnostiach, ktoré by mohli mať vplyv na vznik/platnosť previerky.

15. Posúdenie, ktoré sa má vykonať pred vydaním FSC, musí byť v súlade s požiadavkami a kritériami stanovenými v podpornej smernici o utajovaných projektoch a priemyselnej bezpečnosti popri platných národných zákonoch a predpisoch.

16. Uchádzač, ktorý nemá príslušné FSC, ako to požaduje potenciálna zmluva alebo subdodávateľská zmluva, nebude automaticky vylúčený z výberového konania. Verejný obstarávateľ musí vynaložiť všetko úsilie na obmedzenie stupňa utajenia utajovaných skutočností, ktoré majú byť poskytnuté uchádzačom na najnižšiu možnú úroveň, ktorá ešte umožňuje informovanú a kvalifikovanú odpoveď na výzvu na predkladanie ponúk. V súťažných podkladoch sa však musí oznámiť požiadavka príslušného FSC pred uzatvorením zmluvy/subdodávateľskej zmluvy.

17. Scenáre identifikujúce požiadavky FSC sú uvedené v podpornej smernici o utajovaných projektoch a priemyselnej bezpečnosti.

18. FSC alebo PSC sa nevyžaduje pri zmluvách alebo prístupu k utajovaným skutočnostiam so stupňom utajenia NR. Krajina, ktorá podľa svojich národných bezpečnostných zákonov a predpisov vyžaduje FSC pre zmluvu alebo subdodávateľskú zmluvu so stupňom utajenia NR, nesmie diskriminovať dodávateľa z krajiny, ktorá nevyžaduje FSC, ale zabezpečí, aby bol dodávateľ informovaný o svojich povinnostiach v súvislosti s ochranou utajovaných skutočností a získa od neho potvrdenie, že tieto povinnosti berie na vedomie.

Bezpečnostné previerky osôb pre zamestnancov podnikateľského subjektu

19. Zamestnanci podnikateľského subjektu, ktorí sa majú oboznamovať s utajovanými informáciami stupňa utajenia NC alebo vyšším, musia mať príslušnú PSC. Vydávanie PSC musí byť v súlade s prílohou C k CM(2002)49, smernicou o personálnej bezpečnosti a smernicou o utajovaných projektoch a priemyselnej bezpečnosti.

20. Žiadosti o vykonanie bezpečnostných previerok pre zamestnancov podnikateľského subjektu dodávateľa budú podané na NSA/DSA, ktorý je zodpovedný za podnikateľský subjekt. Pri predkladaní žiadosti o overenie alebo o vykonanie PSC musí podnikateľský subjekt stanoviť stupeň utajovaných skutočností NATO, ku ktorým má zamestnanec prístup.

21. Ak chce podnikateľský subjekt zamestnať občana nečlenskej krajiny NATO na pozíciu, ktorá si vyžaduje prístup k utajovaným skutočnostiam NATO, je zodpovednosťou NSA/DSA krajiny, pod ktorej jurisdikciu spadá podnikateľský subjekt, ktorý zamestnáva, aby vykonal bezpečnostnú previerku tak, ako je ustanovené v tomto dokumente, a určil, že osoba môže získať prístup v súlade s požiadavkami prílohy C, smernicou o personálnej bezpečnosti a smernice o utajovaných projektoch a priemyselnej bezpečnosti.

UVOĽNENIE UTAJOVANÝCH SKUTOČNOSTÍ NATO PRI UZATVÁRANÍ ZMLÚV

22. Uvoľnenie utajovaných skutočností NATO pri uzatváraní zmlúv môže mať buď formu uvoľnenia nečlenským krajinám NATO a medzinárodným organizáciám, alebo uvoľnenie neprogramovým/projektovým účastníkom z členských krajín NATO. Uvoľnenie musí byť so súhlasom príslušného NPA/NPO a/alebo pôvodcu, a v súlade s ostatnými príslušnými prílohami Bezpečnostnej politiky NATO, smernice o administratívnej bezpečnosti, ako aj smernice o utajovaných projektoch a priemyselnej bezpečnosti.

MANIPULOVANIE S UTAJOVANÝMI SKUTOČNOSŤAMI NATO V KOMUNIKAČNÝCH A INFORMAČNÝCH SYSTÉMOCH (CIS)

23. Na ukladanie, spracovanie alebo prenos (ďalej len ako „manipulácia“) utajovaných informácií NATO môžu byť použité iba náležite bezpečnostne akreditované CIS. Príloha F k C-M(2002)49, „Primárna smernica o bezpečnosti CIS“ (AC/35-D/2004), „Smernica o manažmente INFOSEC pre CIS“ (AC/35-D/2005) a všetky relevantné technické a implementačné smernice o bezpečnosti CIS (dokumenty AC/322) poskytujú ďalšiu politiku a usmernenia pre konformnú implementáciu CIS, ktoré manipulujú s utajovanými skutočnosťami NATO.

24. Bezpečnostná akreditácia CIS spracovania utajovaných skutočností NR môže byť delegovaná na dodávateľov v súlade s národnými zákonmi a nariadeniami. Pri aplikácii takéhoto delegovania si ponechávajú príslušné NSA/DSA/SAA zodpovednosť za ochranu utajovaných skutočností so stupňom utajenia NR, s ktorými zaobchádza dodávateľ, a právo na kontrolu bezpečnostných opatrení prijatých dodávateľmi. Okrem toho poskytuje dodávateľ verejnému obstarávateľovi a, ak je to vhodné, bezpečnostnému orgánu stanovenému v smernici o utajovaných projektoch a priemyselnej bezpečnosti vyhlásenie o zhode, ktorým potvrdzuje, že CIS, ktorý sa používa na spracovanie utajovaných skutočností so stupňom utajenia NR, bol akreditovaný v súlade s politikou bezpečnosti v rámci NATO a jej podpornými smernicami o bezpečnosti CIS.

POSTUPY KONTROLY MEDZINÁRODNÝCH NÁVŠTEV (IVCP)

25. IVCP sa vzťahujú na medzinárodné návštevy zástupcov členských krajín NATO, civilných a vojenských orgánov NATO, dodávateľov a subdodávateľov, ktoré zahŕňajú utajované skutočnosti NATO. Týkajú sa aj zástupcov nečlenskej krajiny NATO, vrátane dodávateľov/subdodávateľov takejto krajiny, ak takáto krajina prijala IVCP.

26. Návštevy, ktoré zahŕňajú prístup k utajovaným skutočnostiam NATO so stupňom utajenia NC a vyšším alebo prístup bez sprievodu do bezpečnostných oblastí, musí schváliť NSA/DSA. Návštevy týkajúce sa prístupu k utajovaným skutočnostiam NU[2] alebo NR môžu byť dohodnuté priamo medzi vysielajúcim a prijímajúcim subjektom bez formálnych požiadaviek.

27. Podrobné spôsoby vykonávania medzinárodných návštev sú stanovené v smernici o utajovaných projektoch a priemyselnej bezpečnosti.

PREPOŽIČANIE PERSONÁLU V RÁMCI PROJEKTU/PROGRAMU NATO

28. V prípade, že osoba, ktorá bola bezpečnostne preverená na prístup k utajovaným skutočnostiam NATO, sa má prepožičať z jedného subjektu do druhého v rámci rovnakého programu/projektu NATO, ale v odlišnej členskej krajine NATO, subjekt materskej krajiny prepožičiavanej osoby požiada svoj NSA/DSA o vydanie certifikátu personálnej bezpečnosti osoby pre NSA/DSA subjektu, ktorému sa má osoba prepožičať. Prepožičaná osoba sa príjme použitím postupov žiadosti o povolenie medzinárodnej návštevy, ktoré sú stanovené v smernici o utajovaných projektoch a priemyselnej bezpečnosti a v súlade so zákonmi a nariadeniami o národnej bezpečnosti.

2 NU nie je bezpečnostný stupeň utajenia NATO

MEDZINÁRODNÝ PRENOS A PREPRAVA UTAJOVANÉHO MATERIÁLU NATO

Bezpečnostné princípy platné pre všetky formy prepravy

29. Pri skúmaní navrhovaných bezpečnostných opatrení pre medzinárodnú prepravu zásielok utajovaných skutočností musia byť uplatnené nasledujúce zásady:

a) bezpečnosť sa zabezpečuje vo všetkých etapách počas prepravy a za každých okolností od miesta pôvodu do konečného miesta určenia,

b) stupeň ochrany poskytnutý zásielke sa určí podľa najvyššej úrovne utajenia materiálu obsiahnutého v zásielke,

(c) tam, kde je to možné sa od spoločnosti zabezpečujúcej prepravu vyžaduje FSC. V takýchto prípadoch sa personálu, ktorý manipuluje so zásielkou, vystavuje PSC v súlade s ustanoveniami tejto prílohy,

(d) trasy sa naplánujú z jedného bodu do druhého čo najdetailnejšie, a musia byť vykonané tak rýchlo, ako to okolnosti umožňujú, a

(e) je potrebné dbať na to, aby trasa viedla len cez členské krajiny NATO. Trasy cez krajiny, ktoré nie sú členmi NATO, sa môžu vykonávať iba s povolením NSA/DSA, ktorý má jurisdikciu nad odosielateľom a v súlade s podpornou smernicou o administratívnej bezpečnosti.

30. Opatrenia pre zásielky s utajovanými skutočnosťami musia byť stanovené pre každý program/projekt. Takéto opatrenia však musia zabezpečiť, aby neexistovala pravdepodobnosť neoprávneného prístupu k utajovanému materiálu.

31. Bezpečnostné štandardy pre medzinárodnú prepravu utajovaných materiálov NATO možno nájsť v podpornej smernici o administratívnej bezpečnosti. Podrobné požiadavky na osobnú prepravu utajovaných skutočností NATO, prepravu utajovaných skutočností komerčnými kuriérskymi spoločnosťami, bezpečnostnou službou a sprievodom a na prepravu výbušnín, pohonných hmôt alebo iných nebezpečných látok sú stanovené v podpornej smernici o utajovaných projektoch a priemyselnej bezpečnosti.

SLOVNÍK
POJMOV k
C-M(2002)49

SLOVNÍK POJMOV

Účtovateľné Informácie	Všetky utajované skutočnosti so stupňom utajenia CTS a NS a všetky utajované skutočnosti špeciálnej kategórie (ako ATOMAL).
Hodnovernosť	Hodnovernosť je akt overovania prezentovanej identity subjektu.
Dostupnosť	Vlastnosť informácie a veci umožňujúca jej dostupnosť a použitie na základe požiadavky oprávnenej osoby alebo subjektu.
Porušenie bezpečnosti	Konanie alebo opomenutie, úmyselné alebo z nedbanlivosti, v rozpore s bezpečnostnou politikou NATO a podpornými smernicami, ktoré vedú ku skutočnému alebo možnému ohrozeniu utajovaných skutočností NATO alebo podporných služieb a zdrojov (vrátane napríklad utajovaných skutočností, ktoré sa stratili pri preprave, utajovaných skutočností ponechaných v nezabezpečenej oblasti, kde majú prístup nepreverené osoby bez sprievodu, účtovateľný dokument, ktorý nie je možné nájsť, utajované skutočnosti, ktoré boli vystavené neoprávnenej zmene, zničené neoprávneným spôsobom alebo v prípade CIS nastane odopretie služby.
Utajovaná skutočnosť	Akákoľvek informácia (konkrétne vedomosť, ktorá môže byť sprostredkovaná v akejkoľvek forme) alebo vec, ktorá je predmetom ochrany pred neoprávneným zverejnením, a bola takto označená príslušným stupňom utajenia.
Bezpečnosť komunikačných a informačných systémov (Bezpečnosť CIS)	Uplatňovanie bezpečnostných opatrení na ochranu komunikačných, informačných a iných elektronických systémov a informácií, ktoré sú v týchto systémoch uložené, spracovávané alebo prenášané s ohľadom na dôvernosť, integritu, dostupnosť, hodnovernosť a nespochybniteľnosť.
Kompetentný orgán	Orgán určený NSA členskej krajiny NATO, ktorý je oprávnený vykonávať personálne bezpečnostné previerky s cieľom poskytnúť svojim štátnym príslušníkom prístup k utajovaným skutočnostiam NATO.
Zneužitie	Zneužitie označuje situáciu, keď kvôli porušeniu bezpečnosti alebo nepriateľskej činnosti (napríklad špionáž, teroristické činy**,** sabotáž alebo krádež), utajované skutočnosti NATO stratili svoju dôvernosť, integritu alebo dostupnosť alebo podporné služby a zdroje stratili svoju integritu alebo dostupnosť. Zahŕňa to stratu, sprístupnenie nepovolaným osobám (napr. prostredníctvom špiónáže alebo médiám), neoprávnenú úpravu, zničenie neoprávneným spôsobom alebo odopretie služby.
Dôvernosť	Vlastnosť, ktorá určuje, že informácie nie sú sprístupnené alebo zverejnené neoprávneným osobám alebo subjektom.
Príjemca	Dodávateľ, zariadenie alebo iná organizácia prijímajúca materiál od odosielateľa.
Odosielateľ	Dodávateľ, zariadenie alebo iná organizácia zodpovedná za zorganizovanie odoslania materiálu.
Zmluva	Právne vynútiteľná dohoda o poskytnutí tovarov alebo služieb.

Február 2013
Doplnok č. 9

Dodávateľ	Priemyselný, obchodný alebo iný subjekt, ktorý súhlasí s poskytnutím tovarov alebo služieb.
Kuriér	Osoba oficiálne určená na osobnú prepravu materiálu.
Šifrový materiál	Zahŕňa šifrovacie algoritmy a šifrovacie hardvérové a softvérové moduly a produkty vrátane implementačných detailov a súvisiacej dokumentácie a kľúčového materiálu (pre symetrické aj asymetrické šifrovacie mechanizmy).
Určená bezpečnostná autorita (DSA)	Orgán, ktorý zodpovedá Národnému bezpečnostnému úradu (NSA) členskej krajiny NATO, zodpovedný za komunikáciu s priemyslom v oblasti národnej politiky pre všetky oblasti politiky priemyselnej bezpečnosti NATO a za poskytnutie usmernenia a pomoci s jej implementácii. V niektorých krajinách môže funkciu DSA vykonávať NSA.
Dokument	Akákoľvek zaznamenaná informácia, bez ohľadu na jej fyzickú formu alebo charakter, vrátane, ale nie len, písaných alebo tlačených údajov, kariet a pások na záznam údajov, máp, tabuliek, fotografií, malieb, kresieb, rytín, nákresov, pracovných poznámok a papierov, kópií z kopírovacích papierov alebo atramentových pások alebo reprodukcií vyrobených akýmikoľvek prostriedkami alebo postupmi, hlasových, zvukových, magnetických, elektronických, optických alebo obrazových záznamov v akejkoľvek forme, prenosných zariadení automatického spracovania dát s príslušným počítačovým pamäťovým médiom a prenosných počítačových pamäťových médií.
Dynamické riadenie rizika	Schopnosť vykonávať riadenie rizík takým spôsobom, aby sa neustále posudzovalo riziko používania CIS, akákoľvek zmena v súvislosti s prevádzkou CIS, sa dynamicky premietne do podpisu rizika a včasného uplatňovania protiopatrení týkajúcich sa bezpečnosti, ktoré sú najvhodnejšie pre danú situáciu.
Sprievod	Ozbrojení alebo neozbrojení príslušníci národnej polície, armády alebo iného štátneho orgánu. Ich úlohou je zabezpečiť bezpečný pohyb materiálu, ale nemajú priamu zodpovednosť za predmet ochrany samotného materiálu.
Zariadenie	Inštalácia, závod, továreň, laboratórium, kancelária, univerzita alebo iná vzdelávacia inštitúcia alebo obchodný podnik, vrátane akýchkoľvek pridružených skladov, skladovacích priestorov, zariadení a komponentov, ktoré z pohľadu fungovania a umiestnenia tvoria prevádzku právnickej osoby.
Previerka priemyselnej bezpečnosti (FSC)	Úradné vyjadrenie NA/DSA, že z hľadiska bezpečnosti si môže subjekt dovoliť primeranú bezpečnostnú ochranu pre utajované skutočnosti NATO konkrétneho alebo nižšieho stupňa utajenia, a že jeho personál, ktorý vyžaduje prístup k utajovaným skutočnostiam NATO, bol riadne preverený a poučený o bezpečnostných požiadavkách NATO potrebných na konanie na utajovaných kontraktoch NATO.
Stráže	Civilní (štátni zamestnanci alebo zamestnanci zúčastneného dodávateľa) alebo vojenskí pracovníci, ktorí môžu byť ozbrojení alebo neozbrojení. Môžu byť pridelení iba pre bezpečnostné povinnosti alebo môžu kombinovať povinnosti bezpečnostnej stráže s inými povinnosťami.

Hostiteľská krajina	Všeobecne: Krajina, v ktorej sa nachádza civilný alebo vojenský orgán NATO. Priemyselná bezpečnosť: krajina určená oficiálnym orgánom NATO, ktorý bude vystupovať ako vládna agentúra na uzatváranie zmlúv o plnení hlavnej zmluvy NATO. Krajiny, v ktorých sa plnia subdodávky, sa nenazývajú hostiteľskými krajinami.
Informácie	Poznatky, ktoré môžu byť sprostredkované v akejkoľvek forme.
Zabezpečenie informácií	Informácie sa chránia uplatňovaním zásady zabezpečenia informácií, ktorá je opísaná ako súbor opatrení na dosiahnutie danej úrovne dôvery v ochranu komunikačných, informačných a iných elektronických systémov, neelektronických systémov a informácií, ktoré sú uložené, spracovávané alebo prenášané v týchto systémoch s ohľadom na dôvernosť, integritu, dostupnosť, nespochybniteľnosť a autentifikáciu/hodnovernosť.
Priestupok	Bezpečnostný priestupok je konanie alebo opomenutie, úmyselné alebo z nedbanlivosti, v rozpore s Bezpečnostnou politikou NATO a podpornými smernicami, ktoré nevedú k skutočnému alebo možnému zneužitiu utajovaných informácií NATO (napr. utajované skutočnosti NATO ponechané nezabezpečené vo vnútri zabezpečeného priestoru, kde sú všetky osoby primerane preverené, nezabezpečenie dvojitého zabalenia utajovaných skutočností, atď.).
Integrita	Vlastnosť, že informácia (vrátane údajov, ako je šifrovací text) nebola zmenená alebo zničená neoprávneným spôsobom.
Medzinárodné návštevy	Návštevy osôb podliehajúcich jednému NSA/DSA alebo patriace orgánu NATO, do zariadení alebo orgánov podliehajúcim inému NSA/DSA alebo NATO, ktoré budú vyžadovať alebo môžu obnášať prístup k utajovaným skutočnostiam NATO, alebo kde bez ohľadu na to, či príslušná úroveň utajenia, vnútroštátne právne predpisy, ktorými sa riadi zariadenie alebo orgán, ktorý sa má navštíviť na podporu súvisiacich činností schválených NATO, si vyžadujú, aby takéto návštevy schválil príslušný NSA/DSA. Všetky civilné a vojenské orgány NATO patria do bezpečnostnej jurisdikcie NATO.
Životný cyklus	Životný cyklus informácií zahŕňa fázy plánovania, zhromažďovania, tvorby alebo generovania informácií, ich organizáciu, vyhľadávanie, používanie, dostupnosť a prenos, ich ukladanie a ochranu, a nakoniec, ich vyradenie prostredníctvom prenosu do archívu alebo zničením.
Významný program/projekt	Program alebo projekt veľkého významu, zvyčajne zahŕňajúci viac než dve krajiny a bezpečnostné opatrenia, ktoré presahujú bežné základné požiadavky opísané v bezpečnostnej politike NATO.
Materiál	Materiál zahŕňa dokumenty a taktiež akékoľvek súčasť mechanizmu, zariadení/komponentov, zbraní alebo nástrojov či už vyrobených alebo v procese výroby.
Štátni príslušníci	Štátni príslušníci zahŕňajú „štátnych príslušníkov kráľovstva“, „občanov štátu“ a „prisťahovalcov na území Kanady“. „Prisťahovalci na území Kanady“ sú osoby, ktoré prešli národným procesom preverovania, vrátane kontroly pobytu, registrov trestov a bezpečnostných kontrol a ktorí získajú zákonné povolenie na zriadenie trvalého pobytu v krajine.

Národný bezpečnostný úrad (NSA)	Orgán členskej krajiny NATO zodpovedný za dodržiavanie bezpečnosti utajovaných skutočností NATO v štátnych orgánoch a útvaroch, vojenských alebo civilných, doma alebo v zahraničí.
NATO	„NATO“ označuje Organizáciu Severoatlantickej zmluvy a orgány riadiace sa buď Dohodou o štatúte Organizácie Severoatlantickej zmluvy, národných predstaviteľov a Medzinárodného štábu, podpísanou v Ottawe 20. septembra 1951, alebo Protokolom o štatúte Hlavného medzinárodného vojenského veliteľstva, zriadeného na základe Severoatlantickej zmluvy, podpísanej v Paríži 28. augusta 1952.
Utajovaný kontrakt NATO	Každá zmluva vydaná civilným alebo vojenským orgánom NATO alebo členským štátom NATO na podporu programu alebo projektu financovaného alebo spravovaného NATO, ktorý bude vyžadovať prístup k utajovaným skutočnostiam NATO alebo bude takéto utajované skutočnosti vytvárať.
Utajovaná skutočnosť NATO	a) informácia je definovaná ako poznatok, ktorý môže byť sprostredkovaný akoukoľvek formou, b) utajovaná skutočnosť je definovaná ako informácia alebo vec, ktorá je predmetom ochrany pred neoprávneným zverejnením, a bola takto označená príslušným stupňom utajenia, c) slovo „materiál/vec“ zahŕňa dokumenty a taktiež akúkoľvek súčasť mechanizmu, zariadenia, alebo zbraní či už vyrobených alebo v procese výroby, d) slovo „dokument“ znamená akúkoľvek zaznamenanú informáciu, bez ohľadu na jej fyzickú formu alebo charakter, vrátane, ale nielen, písaných alebo tlačených materiálov, údajov, kariet a pások na záznam údajov, máp, tabuliek, fotografií, malieb, kresieb, rytín, nákresov, pracovných poznámok a papierov, kópií z kopírovacích papierov alebo atramentových pások alebo reprodukcií vyrobených akýmikoľvek prostriedkami alebo postupmi, hlasových, zvukových, magnetických, elektronických, optických alebo obrazových záznamov v akejkoľvek forme, prenosných IT zariadení
Vojenský výbor NATO (NAMILCOM)	Najvyšší vojenský orgán v NATO; NAMILCOM je zodpovedný za celkové vedenie vojenských záležitostí. NAMILCOM je zodpovedný za schvaľovanie a určovanie priorít z operačného hľadiska, požiadaviek používateľov, predkladaných veliteľmi zo strategického velenia.
Previerka personálnej bezpečnosti NATO	Určenie, či je osoba oprávnená na prístup k utajovaným skutočnostiam NATO.
Organizácia NATO pre výrobu a logistiku (NPLO)	Pridružený orgán vytvorený v rámci NATO na plnenie úloh vyplývajúcich zo zmluvy, ktorému Severoatlantická rada udeľuje jasne definovanú organizačnú, administratívnu a finančnú nezávislosť. Skladá sa z predstavenstva a výkonného orgánu, zloženého z generálneho riaditeľa a personálu.
Program NATO	Program schválený Radou, ktorý spravuje manažment/kancelária NATO podľa predpisov NATO.
Projekt NATO	projekt schválený Radou, ktorý spravuje manažment/kancelária NATO podľa predpisov NATO.

Február 2013
Doplnok č. 9

Agentúra projektového manažmentu NATO	Výkonný orgán NPLO.
Need-to-know	Pozrite bod „princíp need-to-know“
Rokovania	Tento pojem zahŕňa všetky aspekty zadávania zákazky alebo subdodávky od počiatočného „oznámenia o zámere na výzvu na predloženie ponúk“ až po konečné rozhodnutie o uzatvorení zmluvy alebo zmluvy o subdodávke.
Nespochybniteľnosť	Opatrenie na uistenie príjemcu preukazujúce odoslanie informácie konkrétnou osobou alebo organizáciou a na uistenie odosielateľa preukazujúce prijatie informácie zadaným príjemcom.
Otvorený skladový priestor	Oblasť postavená v súlade s bezpečnostnými požiadavkami a odsúhlasená vedúcim civilného alebo vojenského orgánu na otvorené ukladanie utajovaných skutočností.
Pôvodca	Krajina alebo medzinárodná organizácia, pod ktorej autoritou boli informácie vytvorené alebo zavedené do NATO.
Materská krajina	Kráľovstvo alebo štát, ktorého je osoba štátnym príslušníkom alebo občanom.
Materský národný bezpečnostný úrad (NSA)	NSA kráľovstva alebo štátu, ktorého je osoba štátnym príslušníkom alebo občanom.
Previerka personálnej bezpečnosti (PSC)	Určenie, že osoba je oprávnená na prístup k utajovaným skutočnostiam.
Hlavná zmluva	Počiatočná zmluva vedená agentúrou projektového manažmentu/kanceláriou NATO pre program/projekt.
Hlavný dodávateľ	Priemyselný, obchodný alebo iný subjekt členskej krajiny, ktorý uzavrel zmluvu s Agentúrou projektového manažmentu/kanceláriou NATO pre riadenie projektov na vykonanie služby alebo výrobu výrobku v rámci projektu NATO a ktorý môže zasa uzatvárať zmluvy so subdodávateľmi na základe schválenia.
Princíp need-to-know	Princíp, podľa ktorého sa kladne určí, že potenciálny príjemca potrebuje mať prístup k, vedomosť o, alebo držbu informácie za účelom plnenia svojich oficiálnych úloh alebo služieb.
Príručka k bezpečnostnému utajeniu projektu/programu	Časť bezpečnostných inštrukcií (PSI) programu/projektu, ktorá identifikuje časti programu, ktoré sú utajované, špecifikujúc úrovne bezpečnostného stupňa utajenia. Príručka k bezpečnostnému utajeniu môže byť rozširovaná počas celého životného cyklu programu a utajené časti informácií sa môžu prehodnocovať z hľadiska utajenia – prehodnotením lehoty utajenia alebo znížením stupňa utajenia.
Bezpečnostné inštrukcie k programu/projektu (PSI)	Kompilácia bezpečnostných nariadení/postupov, založená na bezpečnostnej politike NATO a podporných smerniciach, ktoré sa uplatňujú na konkrétny projekt/program s cieľom štandardizovať bezpečnostné postupy. PSI tiež predstavuje prílohu k hlavnej zmluve a môžu byť revidované počas celého životného cyklu programu. V prípade subdodávateľských zmlúv uzatvorených v rámci PSI predstavuje základ pre SAL.

Riziko	Pravdepodobnosť, že zraniteľnosť bude úspešne využitá hrozbou, čo vedie k zneužitiu dôvernosti, integrity a/alebo dostupnosti a k spôsobeniu ujmy.
Riadenie rizík	Systematický prístup k určeniu bezpečnostných protiopatrení potrebných na ochranu informácií a podporných služieb a zdrojov na základe hodnotenia hrozieb a zraniteľných miest. Riadenie rizík zahŕňa plánovanie, organizovanie, riadenie a kontrolu zdrojov, aby sa zabezpečilo, že riziko zostane v rámci akceptovateľných hraníc.
Bezpečnostné listy (SAL)	Dokument vydaný príslušným orgánom ako súčasť ktorejkoľvek utajovanej zmluvy alebo subdodávateľskej zmluvy NATO, okrem hlavných programov/projektov, ktorý identifikuje bezpečnostné požiadavky alebo ich prvky, ktoré si vyžadujú bezpečnostnú ochranu.
Bezpečnostná záruka	Záruka poskytnutá NATO buď priamo alebo prostredníctvom členskej krajiny NATO alebo civilného alebo vojenského orgánu NATO, sponzorujúceho uvoľnenie, o tom, že príjemca utajovaných skutočností NATO z nečlenskej krajiny NATO, im poskytne rovnakú úroveň ochrany, aká je vyžadovaná bezpečnostnou politikou NATO.
Kontrolný zoznam stupňov utajenia	Súčasť bezpečnostného listu (SAL), ktorá opisuje prvky zmluvy, ktoré sú utajované, špecifikujúc bezpečnostné stupne utajenia. V prípade zmlúv uzavretých v rámci programu/projektu vyplývajú tieto prvky informácií z bezpečnostných pokynov programu (projektu) vydaných pre daný program.
Utajovaná skutočnosť špeciálnej kategórie	Informácie ako napríklad ATOMAL alebo informácie jednotného integrovaného operačného plánu (SIOP), na ktoré sa vzťahujú dodatočné postupy manipulácie /ochrany.
Subdodávateľská zmluva	Zmluva uzatvorená hlavným dodávateľom s iným dodávateľom (t. j. subdodávateľom) na dodanie tovarov alebo služieb.
Subdodávateľ	Dodávateľ, s ktorým hlavný dodávateľ uzatvorí subdodávateľskú zmluvu.
Hrozba	Možnosť zneužitia, straty alebo krádeže utajovaných skutočností NATO alebo podporných služieb a zdrojov. Hrozba môže byť definovaná na základe svojho pôvodu, motivácie alebo výsledku, môže byť úmyselná alebo nedbanlivostná, násilná alebo skrytá, externá alebo interná.
Zraniteľnosť	Slabá stránka, atribút alebo nedostatok kontroly, ktorá by umožnila alebo uľahčila spustenie hrozby voči utajovaným skutočnostiam NATO alebo podporným službám a zdrojom.