



KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, den 27.10.2008  
KOM(2008) 676 endelig

2008/0200 (CNS)

Forslag til

**RÅDETS BESLUTNING**

**om et informations- og varslingsnetværk vedrørende kritisk infrastruktur (CIWIN)**

{SEC(2008)2701}  
{SEC(2008)2702}

(forelagt af Kommissionen)

## **BEGRUNDELSE**

### **BAGGRUNDEN FOR FORSLAGET**

#### **Begrundelse og formål**

På Det Europæiske Råds møde i juni 2004 blev Kommissionen anmodet om at udforme en overordnet strategi for beskyttelse af kritisk infrastruktur. Den 20. oktober 2004 vedtog Kommissionen en meddelelse vedrørende beskyttelse af kritisk infrastruktur i forbindelse med bekæmpelse af terrorisme, der indeholder forslag til, hvordan EU kan forbedre forebyggelsen, beredskabet og reaktionen i forbindelse med terrorangreb, der påvirker kritisk infrastruktur. Det Europæiske Råd gav i sine konklusioner af december 2004 vedrørende forebyggelse, beredskab og reaktion i forbindelse med terrorangreb og i EU's solidaritetsprogram om følgerne af terrortrusler og –angreb sin støtte til, at Kommissionen fremsætter et forslag til et europæisk program for beskyttelse af kritisk infrastruktur (EPCIP) og var enig i, at Kommissionen skulle oprette et informations- og varslingsnetværk vedrørende kritisk infrastruktur (CIWIN).

I december 2006 fremsatte Kommissionen et forslag til direktiv om indkredsning og klassificering af europæisk kritisk infrastruktur, og en vurdering af behovet for at beskytte det. Samtidig udsendte Kommissionen en meddelelse om EPCIP-programmet. Disse dokumenter danner tilsammen rammerne for beskyttelse af infrastruktur i EU. I meddelelsen fastsættes de generelle rammer for beskyttelse af kritisk infrastruktur i EU, og det forklares hvordan EPCIP-programmet (herunder informations- og varslingsnetværket) kan gennemføres.

Initiativet vedrørende et informations- og varslingsnetværk er en del af EPCIP-programmet og vedrører specielt informationsdeling mellem EU-medlemsstaterne og det it-system, der skal understøtte dette.

#### **Generel baggrund**

EU's sikkerhed og økonomi såvel som EU-borgernes velfærd afhænger af bestemte former for infrastruktur og de tjenester, de leverer. F.eks. er telekommunikations- og energinettene, finansielle tjenesteydelser og transportsystemer, sundhedsvæsenet og forsyningen af rent drikkevand og mad vigtige for EU og EU-medlemsstaterne. Ødelæggelse eller afbrydelse af infrastruktur, der leverer nøgledydelser, og en u hensigtsmæssig reaktion herpå kan medføre tab af menneskeliv, ejendom og befolkningens tillid til EU. Den komplekse indbyrdes afhængighed betyder, at en særlig begivenhed kan have en dominoeffekt på andre sektorer og områder, der ikke umiddelbart og tydeligt er indbyrdes forbundne. Der er ikke i tilstrækkelig grad blevet forsket i denne type indbyrdes forbindelse, og resultatet heraf kan blive, at kritisk infrastruktur og sikkerheden for EU-borgerne ikke beskyttes tilstrækkeligt.

Kritisk infrastruktur i EU er på nuværende tidspunkt genstand for en lang række meget forskellige beskyttelsesforanstaltninger og forpligtelser uden generelle fælles minimumsstandarder. Nogle medlemsstater er allerede langt fremme i processen med at indkredse deres nationale kritiske infrastruktur, har indført strenge beskyttelsesforanstaltninger og råder over en lang række former for praksis og strukturer til at sikre beskyttelsen heraf. Andre har først lige indledt denne proces og kan i høj grad have nytte af at få adgang til bedste praksis såsom metoder til at foretage en risikovurdering. Problemet kan ansues geografisk (dvs. mellem medlemsstaterne) og sektorielt (dvs. mellem forskellige sektorer med kritisk infrastruktur).

Det er meget komplekst at tage fat på spørgsmålet om udveksling af oplysninger mellem medlemsstaterne, og det kræver mange overvejelser. Det er vigtigt at undgå overlapninger af aktiviteter som følge af utilstrækkelige oplysninger om lignende situationer i andre medlemsstater. Oplysninger om bedste praksis i én medlemsstat kan f.eks. være med til at forhindre, at der bruges midler på at udvikle en lignende praksis i andre medlemsstater.

Der er desuden blandt de berørte aktører frygt for at udveksle følsomme oplysninger. Hvis der skal sikres en effektiv informationsudveksling, er det nødvendigt at skabe tillid og fleksibilitet.

### **Gældende bestemmelser på det område, som forslaget vedrører**

Der eksisterer på nuværende tidspunkt ingen bestemmelser om udveksling af oplysninger og varslinger på området beskyttelse af kritisk infrastruktur i EU, selv om Kommissionen i 2006 fremsatte forslag til et direktiv om indkredsning og klassificering af europæisk kritisk infrastruktur og en vurdering af behovet for at beskytte det (KOM(2006) 787 endelig). Samtidig udsendte Kommissionen en meddelelse om et europæisk program for beskyttelse af kritisk infrastruktur (EPCIP) (KOM(2006) 786 endelig). I juni 2008 blev der opnået politisk enighed i Rådet om ovennævnte direktiv, og det er planlagt at vedtage det i anden halvdel af 2008.

Derudover findes der i EU en række sektorbaserede systemer for hurtig varsling. Hovedforskellen mellem informations- og varslingsnetværket og de eksisterende systemer til hurtig varsling er, at førstnævnte er tværsektoriel. Ingen af de eksisterende systemer til hurtig varsling har en generel og tværsektoriel funktionalitet, der er tilgængelig for en lang række berørte aktører (relevante nationale myndigheder med ansvar for beskyttelse af kritisk infrastruktur og ministerier m.fl.), men kun for nødtjenester.

- Rådets beslutning om indførelse af Fællesskabets civilbeskyttelsesordning (omarbejdet) (2007/779/EF, Euratom)
- Rådets beslutning om en fællesskabsordning for hurtig udveksling af information i tilfælde af strålingsfare (87/600/Euratom) med henblik på oprettelse af et fællesskabssystem for udveksling af presserende radiologiske informationer
- Rådets direktiv 82/894/EØF af 21. december 1982 om anmeldelse af dyresygdomme inden for Fællesskabet (82/894/EØF)
- Rådets direktiv om foranstaltninger mod indslæbning i Fællesskabet af skadegørere på planter eller planteprodukter og mod deres spredning inden for Fællesskabet (2000/29/EF)
- Europa-Parlamentets og Rådets beslutning om oprettelse af et net til epidemiologisk overvågning af og kontrol med overførbare sygdomme i Fællesskabet (2119/98/EF)
- Europa-Parlamentets og Rådets direktiv om produktsikkerhed i almindelighed (2001/95/EF)
- Europa-Parlamentets og Rådets forordning (EF) om generelle principper og krav i fødevarerlovgivningen, om oprettelse af Den Europæiske Fødevarer sikkerhedsautoritet og om procedurer vedrørende fødevarer sikkerhed (178/2002)

- Kommissionens beslutning om udvikling af et integreret veterinærinformationssystem (2003/623/EF)
- Kommissionens afgørelse om ændring af Kommissionens forretningsorden (2006/25/EF, Euratom).

### **Overensstemmelse med andre EU-politikker og -mål**

Dette forslag er fuldt ud i overensstemmelse med EU's mål, særlig med hensyn til "at bevare og udbygge Unionen som et område med frihed, sikkerhed og retfærdighed, hvor der er fri bevægelighed for personer, kombineret med passende foranstaltninger vedrørende kontrol ved de ydre grænser, asyl, indvandring og forebyggelse og bekæmpelse af kriminalitet".

Det er i overensstemmelse med andre politikker, da det ikke sigter mod at erstatte eksisterende foranstaltninger, men at supplere dem for at forbedre beskyttelsen af europæisk kritisk infrastruktur.

### **HØRING AF INTERESSEREDE PARTER OG KONSEKVENSANALYSE**

#### **Høring af interesserede parter**

##### Høringsmetoder, hovedmålgrupper og respondenternes overordnede profil

Alle relevante aktører er blevet hørt om informations- og varslingsnetværket via og inden for rammerne af høringen vedrørende EPCIP-programmet. Det er sket ved hjælp af følgende:

- Grønbogen om beskyttelse af europæisk kritisk infrastruktur blev vedtaget den 17. november 2005, idet høringsperioden udløb den 15. januar 2006. 22 medlemsstater har officielt svaret på høringen. Ca. 100 repræsentanter for den private sektor er også fremkommet med bemærkninger. I svarene blev der generelt givet støtte til idéen om at oprette informations- og varslingsnetværket.
- Kommissionen har været vært for en række uformelle møder med medlemsstaternes kontaktpunkter for beskyttelse af kritisk infrastruktur (december 2005, februar 2006, december 2006, november 2007, februar 2008, marts 2008).
- Undersøgelse vedrørende oprettelsen af et informations- og varslingsnetværk vedrørende kritisk infrastruktur (CIWIN), som en ekstern kontrahent (Unisys) afsluttede i januar 2008. Som en del af undersøgelsen gennemførte kontrahenten interviews vedrørende informations- og varslingsnetværket i alle 27 medlemsstater.
- Uformelle møder med repræsentanter for den private sektor. Der blev afholdt adskillige uformelle møder med repræsentanter for private virksomheder og erhvervsorganisationer.

##### Sammenfatning af svarene og af, hvordan der er taget hensyn til dem

Selv om grønningen vedrørende EPCIP-programmet var bredere, og de berørte aktører blev hørt om mange aspekter af EPCIP-programmet (f.eks. mål og hovedprincipper for programmet, gennemførelsesfaser), blev der i en del af den fokuseret på informations- og varslingsnetværket.

Reaktionerne på grønbogen om EPCIP-programmet og de løbende drøftelser med alle berørte aktører har haft stor indflydelse på udformningen af forslaget vedrørende oprettelsen af informations- og varslingsnetværket. Oprindeligt havde medlemsstaterne ikke samme syn på oprettelsen af netværket. Nogle gik ind for et kommunikations- og varslingsystem med flere niveauer og med to særskilte funktioner: et system for hurtig varsling og et elektronisk forum for udveksling af idéer og bedste praksis med hensyn til beskyttelse af kritisk infrastruktur. En række medlemsstater gik imidlertid ind for, at informations- og varslingsnetværket kun skulle være et forum, eller at det blev begrænset til at være et system for hurtig varsling, der skulle forbinde medlemsstaterne med Kommissionen. På tidspunktet for høringen var to medlemsstater imod informations- og varslingsnetværket. Da der var forskellige meninger, blev spørgsmålet drøftet med medlemsstaterne på regelmæssige møder mellem kontaktpunkterne for beskyttelse af kritisk infrastruktur. Den endelige udformning af informations- og varslingsnetværket er et resultat af disse drøftelser.

## **Ekspertbistand**

### Relevante videnskabelige områder/eksperter

Der blev indsamlet ekspertise gennem adskillige møder og seminarer i 2006, 2007 og 2008 samt gennem høringsproceduren vedrørende grønbogen om EPCIP-programmet. Der blev indsamlet oplysninger fra alle relevante aktører.

### Anvendte metoder

I marts 2006 indgik Kommissionen en kontrakt, der bl.a. omfattede en feasibility-undersøgelse af informations- og varslingsnetværket, og som havde til formål at indsamle oplysninger om bedste praksis vedrørende beskyttelse af kritisk infrastruktur og at gennemføre interviews med eksperter i medlemsstaterne om kravene til informations- og varslingsnetværket både som et netværk for udveksling af oplysninger og et system for hurtig varsling, idet der blev taget hensyn til de eksisterende infrastrukturer og netværk på nationalt og internationalt plan.

Et andet mål var at skabe en fælles platform for udveksling af oplysninger vedrørende beskyttelse af kritisk infrastruktur.

### Væsentligste organisationer/eksperter, der deltog i høringen

Alle EU-medlemsstater.

### Sammendrag af rådgivning, der er modtaget og anvendt

Det har ikke været nævnt, at der skulle eksistere potentielt alvorlige risici med uoprettelige konsekvenser.

### Offentliggørelse af ekspertrådgivningen

Via bilagene til konsekvensanalysen.

## **Konsekvensanalyse**

Der er allerede inden for EPCIP-pakken blevet opnået enighed om at vedtage et særskilt forslag vedrørende informations- og varslingsnetværket, mere specifikt i Kommissionens

meddelelse om EPCIP-programmet. I forbindelse med konsekvensanalysen blev følgende fire muligheder overvejet:

Mulighed 1: Ingen selvstændig politik. Der vil ikke blive truffet tværfaglige foranstaltninger på europæisk plan, og medlemsstaterne skal individuelt tage hånd om problemet.

Mulighed 2: Informations- og varslingsnetværket som en opgradering af eksisterende systemer for hurtig varsling. Netværket vil i medfør af denne mulighed (der kræver både en funktionel revision af den eksisterende it-arkitektur og ændringer af de eksisterende systemers retsgrundlag) få til opgave at sikre, at de eksisterende systemer for hurtig varsling er interoperable og tilgængelige for forskellige tjenester i EU og medlemsstaternes ministerier. Da det kun vil omfatte funktionen hurtig varsling, vil alle tiltag for at tilføje en platform for udveksling af oplysninger og bedste praksis kræve en ændring af de eksisterende systemer for hurtig varsling, der er ret ressourcekrævende.

Mulighed 3: Informations- og varslingsnetværket som en åben platform for (ikke-sikret) udveksling af oplysninger om beskyttelse af kritisk infrastruktur. Denne mulighed kræver et it-værktøj, der er tilgængeligt for den brede offentlighed og fungerer som et almindeligt websted. Dette vil uden tvivl være med til at skabe større bevidsthed omkring beskyttelse af kritisk infrastruktur i Europa og øge den direkte udveksling af oplysninger mellem de berørte aktører. Da den, der ligger inde med oplysninger og uploader disse, aldrig vil vide, hvem slutbrugeren er, vil det imidlertid i væsentlig grad begrænse den mængde oplysninger, der uploades.

Mulighed 4: Informations- og varslingsnetværket som et frivilligt kommunikations- og varslingssystem med flere niveauer og med to særskilte funktioner: et system for hurtig varsling og et elektronisk forum for udveksling af idéer og bedste praksis med hensyn til beskyttelse af kritisk infrastruktur. Denne mulighed indebærer, at informations- og varslingsnetværket oprettes som et it-redskab for opbevaring og videreformidling af følsomme oplysninger, der er klassificeret op til niveauet "RESTREINT UE ". Netværket vil have to hovedfunktioner: 1) et sikkert forum for udveksling af oplysninger med stor vægt på udveksling af bedste praksis, dialog og tillidsskabende foranstaltninger på EU-plan og 2) et system for hurtig varsling vedrørende kritisk infrastruktur. Medlemsstaterne vil frit kunne benytte hele systemet, en af disse funktioner eller ingen overhovedet.

Mulighed 5: Informations og varslingsnetværket som et kommunikations- og varslingssystem med flere niveauer og med to særskilte funktioner: et system for hurtig varsling og et elektronisk forum for udveksling af idéer og bedste praksis med hensyn til beskyttelse af kritisk infrastruktur. I medfør heraf vil informations- og varslingsnetværket være et obligatorisk system, hvor hver enkelt medlemsstat er forpligtet til at uploade og ajourføre relevante oplysninger regelmæssigt.

Kommissionen har udført den konsekvensanalyse, der er nævnt i arbejdsprogrammet. Mulighed 4 - Informations- og varslingsnetværket som et kommunikations- og varslingssystem med flere niveauer og med to særskilte funktioner: et system for hurtig varsling og et elektronisk forum for udveksling af idéer og bedste praksis vedrørende beskyttelse af kritisk infrastruktur – viste sig klart at være de mest fordelagtige løsninger, når der ses på fordele og ulemper. Denne mulighed medfører, at informations- og varslingsnetværket udgør et sikret sted for udveksling af oplysninger, er med til at opbygge tilliden mellem de berørte aktører og gør det muligt at udveksle varslinger.

Der er vedlagt en kopi af konsekvensanalysen vedrørende informations- og varslingsnetværket.

## **FORSLAGETS RETLIGE ASPEKTER**

### **Resumé af forslaget**

Formålet med den foreslåede foranstaltning er at bistå medlemsstaterne med at udveksle oplysninger om fælles trusler, sårbare områder og hensigtsmæssige foranstaltninger og strategier for at afbøde risiciene i forbindelse med beskyttelse af kritisk infrastruktur.

### **Retsgrundlag**

Forslaget har hjemmel i artikel 308 i traktaten om oprettelse af Det Europæiske Fællesskab og artikel 203 i traktaten om oprettelse af Det Europæiske Atomenergifællesskab.

### **Subsidiaritetsprincippet**

Subsidiaritetsprincippet finder anvendelse, for så vidt som forslaget ikke hører ind under Fællesskabets enekompetence.

Målene med forslaget kan af nedenstående grunde ikke opfyldes på tilfredsstillende vis af medlemsstaterne.

Subsidiaritetsprincippet er overholdt, da de foranstaltninger, der er resultatet af dette forslag, ikke kan gennemføres af nogen enkelt medlemsstat og derfor bedre kan træffes på EU-plan.

Selv om det er hver enkelt medlemsstats ansvar at beskytte kritisk infrastruktur under dens jurisdiktion, kan en platform, der dækker hele EU på tværs af grænserne, og som sikrer, at der står oplysninger til rådighed for alle medlemsstater, der kan have gavn heraf, kun gennemføres på EU-plan.

En indsats på fællesskabsplan vil af nedenstående grunde udgøre et mere effektivt redskab til at nå målene for forslaget.

Ingen medlemsstat kan alene sikre en udveksling af oplysninger eller en hurtig udveksling af varslinger på tværs af EU. Det er derfor tydeligt, at det giver en merværdi at arbejde på EU-plan for at koordinere de informationer, der allerede kan foreligge, men som ikke deles med andre.

Kun en indsats på EU-plan kan sikre, at medlemsstater, der ønsker at dele og modtage oplysninger, behandles ens, at samarbejdet ikke virker diskriminerende rent geografisk for nogle medlemsstater, og at oplysningerne virkelig når frem til dem, der ønsker at modtage dem.

Der er en direkte forbindelse mellem det tværfaglige samarbejde på EU-plan og den nationale sikkerhed. I verden af i dag med indbyrdes afhængighed mellem sektorer på tværs af grænserne både i geografisk og sektoriel betydning kan medlemsstaterne tilbyde andre medlemsstater tjenesteydelser eller kan have indflydelse på leveringen af tjenesteydelser i andre medlemsstater. Der er risiko for, at en medlemsstat kommer til at lide, fordi en anden ikke i tilstrækkelig grad har formået at beskytte infrastrukturen på sit eget område.

Et stadigt større antal infrastrukturer er europæiske, hvilket betyder, at en national strategi alene ikke er tilstrækkelig. Der er et klart behov for at tage fat på en lang række trusler, der kan påvirke kritisk infrastruktur i Europa.

Forslaget er derfor i overensstemmelse med subsidiaritetsprincippet.

### **Proportionalitetsprincippet**

Forslaget er i overensstemmelse med proportionalitetsprincippet af nedenstående grunde.

Forslaget går ikke videre end, hvad der er nødvendigt for at nå de bagvedliggende mål for medlemsstaternes samarbejde på området, navnlig med hensyn til medlemsstaternes vilje til at deltage. Den foreslåede foranstaltning gør det muligt for medlemsstater, der ikke ønsker at deltage i systemet, at fravælge det.

I lyset af fordelene ved informations- og varslingsnetværket vil det ikke have væsentlige direkte finansielle virkninger på hverken medlemsstaternes eller EU's budget. F.eks. vil udgifterne til vedligeholdelse være på ca. 550 000 EUR om året, men udgifterne ved begivenheder, som det ved hjælp af informations- og varslingsnetværket vil være muligt at forhindre eller begrænse, vil være meget højere.

### **Valg af instrument**

Foreslået instrument: Rådsbeslutning.

Andre midler vil ikke være hensigtsmæssige af følgende grund(e):

For at prototypen af informations- og varslingsnetværket kan blive fuldt driftsklar og tilgængelig for medlemsstaterne, er det nødvendigt med et retsgrundlag herfor. Da genstanden for dette retlige instrument er specifik og ikke generel, er en rådsbeslutning det bedst egnede instrument til at nå dette mål og samtidig forpligte brugerne af systemet (medlemsstaterne og Kommissionen) til at respektere potentielle krav om fortrolighed for så vidt angår de udvekslede oplysninger.

### **BUDGETMÆSSIGE VIRKNINGER**

De budgetmæssige virkninger vurderes i den ledsagende finansieringsoversigt. Programmet om forebyggelse, beredskab og konsekvensstyring i forbindelse med terrorisme og andre sikkerhedsrelaterede risici for perioden 2007-2013 vil bidrage til gennemførelsen af denne beslutning.

### **YDERLIGERE OPLYSNINGER**

#### **Simulering, pilotfase og overgangsperiode**

Der har været, eller der vil blive gennemført, en simulering eller en pilotfase for forslaget.

#### **Fornyset gennemgang/revision/udløbsklausul**

Forslaget indeholder en klausul om fornyet gennemgang.

Forslaget indeholder en klausul om revision.

Forslag til

## RÅDETS BESLUTNING

### om et informations- og varslingsnetværk vedrørende kritisk infrastruktur (CIWIN)

RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 308,

under henvisning til traktaten om oprettelse af Det Europæiske Atomenergifællesskab, særlig artikel 203,

under henvisning til forslag fra Kommissionen<sup>1</sup>,

under henvisning til udtalelse fra Europa-Parlamentet<sup>2</sup>, og

ud fra følgende betragtninger:

- (1) Det Europæiske Råd gav i sine konklusioner af december 2004 vedrørende forebyggelse, beredskab og reaktion i forbindelse med terrorangreb og EU's solidaritetsprogram om følgerne af terrortrusler og –angreb sin støtte til, at Kommissionen fremsætter et forslag til et europæisk program for beskyttelse af kritisk infrastruktur og var enig i, at Kommissionen skal oprette et informations- og varslingsnetværk vedrørende kritisk infrastruktur (CIWIN)<sup>3</sup>.
- (2) I november 2005 vedtog Kommissionen en grøn bog om et europæisk program for beskyttelse af kritisk infrastruktur (EPCIP), hvori der redegøres for de muligheder, Kommissionen har for at fastlægge, hvad der udgør kritisk infrastruktur, og hvordan der kan oprettes et informations- og varslingsnetværk vedrørende beskyttelse af kritisk infrastruktur. Resultaterne af høringen vedrørende grøn bogen bekræftede interessen blandt de fleste medlemsstater for at oprette et informations- og varslingsnetværk vedrørende kritisk infrastruktur.
- (3) I december 2006 vedtog Kommissionen en meddelelse om et europæisk program for beskyttelse af kritisk infrastruktur (EPCIP)<sup>4</sup>, hvori det blev annonceret, at informations- og varslingsnetværket ville blive oprettet ved hjælp af et særskilt forslag fra Kommissionen, og at det skulle udgøre en platform for sikker udveksling af bedste praksis.

---

<sup>1</sup> EUT C af ....., s. ...

<sup>2</sup> EUT C af ....., s. ...

<sup>3</sup> 14894/04.

<sup>4</sup> KOM(2006) 786 endelig.

- (4) Flere begivenheder i forbindelse med kritisk infrastruktur i Europa såsom det europæiske blackout i 2006 viste, at der er behov for en bedre og mere effektiv udveksling af oplysninger for at forhindre sådanne begivenheder eller begrænse deres omfang.
- (5) Det er hensigtsmæssigt at oprette et informationssystem, der vil sætte medlemsstaterne og Kommissionen i stand til at udveksle oplysninger og varslinger på området beskyttelse af kritisk infrastruktur, at styrke deres dialog herom og bidrage til at fremme integrationen og en bedre koordinering af nationalt spredte og opsplittede forskningsprogrammer vedrørende beskyttelse af kritisk infrastruktur.
- (6) Informations- og varslingsnetværket bør bidrage til at forbedre beskyttelsen af kritisk infrastruktur i EU ved at sikre medlemsstaterne et informationssystem, der kan lette deres samarbejde og udgøre et effektivt og hurtigt alternativ til tidskrævende metoder til at søge efter oplysninger om kritisk infrastruktur i Fællesskabet.
- (7) Informations- og varslingsnetværket bør navnlig fremme udviklingen af hensigtsmæssige foranstaltninger med henblik på at lette udvekslingen af bedste praksis samt udgøre et værktøj til videreformidling af umiddelbare trusler og varslinger på sikker vis.
- (8) Der bør i forbindelse med informations- og varslingsnetværket undgås overlapninger og tages hensyn til særlige kendetegn ved og ekspertise, ordninger og kompetenceområder for hvert af de eksisterende sektorbaserede systemer for hurtig varslingsnetværk.
- (9) Kommissionen har i årenes løb udviklet driftskapaciteten for at kunne bistå i forbindelse med en lang række nødsituationer via adskillige systemer for hurtig varslingsnetværk med sektorspecifikke kendetegn, som er rettet mod specialiserede tjenester inden for EU. De eksisterende systemer for hurtig varslingsnetværk omfatter imidlertid ikke en funktion vedrørende beskyttelse af kritisk infrastruktur, der er tilgængelig for en lang række berørte aktører andre end sektormyndigheder eller nødtjenester.
- (10) Den indbyrdes afhængighed mellem kritisk infrastruktur i medlemsstaterne og de forskellige niveauer for beskyttelse af kritisk infrastruktur i medlemsstaterne tyder på, at det ville øge sikkerheden for borgerne, hvis der blev oprettet et horisontalt og tværsektorielt fællesskabsredskab for udveksling af oplysninger og varslinger vedrørende beskyttelse af kritisk infrastruktur.
- (11) Under hensyntagen til, at kommunikationsnettet "Trans European Services for Telematics between Administrations" (S-TESTA) eller ethvert andet alternativt og sikkert netværk, der drives af Kommissionen, er tilgængeligt fremover, bør Kommissionen træffe beslutning om den mest hensigtsmæssige teknologiske platform for informations- og varslingsnetværket og kræve, at slutbrugerne opfylder de tekniske krav, den har fastsat.
- (12) En forudsætning for, at de relevante berørte parter vil deles om oplysninger om beskyttelse af kritisk infrastruktur, er, at der består et tillidsforhold mellem dem, således at fortrolige eller følsomme oplysninger, som de frivilligt har delt, ikke offentliggøres, og at de følsomme oplysninger beskyttes tilstrækkeligt.

- (13) I overensstemmelse med de fastsatte betingelser, procedurer og sikkerhedsforanstaltninger bør kun autoriserede brugere have adgang til informations- og varslingsnetværket. Brugeradgangen i medlemsstaterne bør begrænses til de kompetente nationale myndigheder, mens adgangen i Kommissionen bør begrænses til de kompetente tjenester.
- (14) Eventuelle udgifter til driften af informations- og varslingsnetværket på fællesskabsplan bør dækkes af fællesskabsmidler og/eller via relevante fællesskabsprogrammer;
- (15) Eventuelle udgifter ved driften af informations- og varslingsnetværket på nationalt plan bør finansieres af medlemsstaterne selv, medmindre andet fastsættes i fællesskabsordninger.
- (16) Da målene for den foranstaltning, der skal iværksættes, nemlig sikker og hurtig udveksling af oplysninger mellem medlemsstaterne, ikke i tilstrækkelig grad kan nås af medlemsstaterne og derfor på grund af foranstaltningens virkninger bedre kan nås på fællesskabsplan, kan Fællesskabet vedtage foranstaltninger i overensstemmelse med subsidiaritetsprincippet, jf. traktatens artikel 5. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne beslutning ikke ud over, hvad der er nødvendigt for at nå disse mål.
- (17) I denne beslutning overholdes de grundlæggende rettigheder og principper, som bl.a. Den Europæiske Unions charter om grundlæggende rettigheder anerkender -

#### VEDTAGET FØLGENDE BESLUTNING:

##### *Artikel 1* *Formål*

I medfør af denne beslutning oprettes der et sikkert informations-, kommunikations- og varslingsystem – informations- og varslingsnetværket vedrørende kritisk infrastruktur (CIWIN) - med henblik på at bistå medlemsstaterne med at udveksle oplysninger om fælles trusler, sårbare områder og hensigtsmæssige foranstaltninger og strategier for at afbøde risiciene i forbindelse med beskyttelse af kritisk infrastruktur.

##### *Artikel 2* *Definitioner*

I denne beslutning forstås ved:

"Kritisk infrastruktur": de aktiver, systemer eller dele heraf i medlemsstaterne, der er vigtige for opretholdelsen af vitale samfundsmæssige funktioner og menneskers sundhed, sikkerhed og økonomiske eller sociale velfærd, og hvis afbrydelse eller ødelæggelse i væsentlig grad ville påvirke en medlemsstat, fordi den som følge heraf ikke ville kunne opretholde disse funktioner.

"Deltagende medlemsstat": de medlemsstater, der har undertegnet et aftalememorandum med Kommissionen.

"CIWIN-repræsentant": kontaktpunkt vedrørende informations- og varslingsnetværket i den relevante medlemsstat eller Kommissionen, der sikrer en hensigtsmæssig anvendelse af informations- og varslingsnetværket og overholdelsen af retningslinjerne for brugere inden for den relevante medlemsstat eller Kommissionen.

"Trussel": ethvert tegn eller enhver omstændighed eller begivenhed, der eventuelt vil kunne afbryde eller ødelægge kritisk infrastruktur eller en del deraf.

### *Artikel 3 Deltagelse*

Alle medlemsstaterne kan deltage i og bruge informations- og varslingsnetværket. Deltagelsen i informations- og varslingsnetværket er betinget af, at medlemsstaterne har undertegnet et aftalememorandum, der indeholder de tekniske og sikkerhedsmæssige krav, der finder anvendelse på informations- og varslingsnetværket, og oplysninger om de lokaliteter, der skal forbindes med informations- og varslingsnetværket.

### *Artikel 4 Funktioner*

- 1) Informations- og varslingsnetværket har følgende to funktioner:
  - a) et elektronisk forum for beskyttelse af kritisk infrastruktur vedrørende informationsudveksling
  - b) en funktion for hurtig varslings, der skal sætte de deltagende medlemsstater og Kommissionen i stand til at sende varslinger om umiddelbare risici og trusler mod kritisk infrastruktur.
- 2) Det elektroniske forum består af permanente underfora og dynamiske underfora.

Permanente underfora er permanent medtaget i systemet. Selv om deres indhold kan tilpasses, kan de ikke fjernes eller omdøbes, og der kan ikke tilføjes nye. Bilag I indeholder en liste over permanente underfora.

Dynamiske underfora oprettes på anmodning og tjener et særligt formål. De ophører med at eksistere, når det oprindelige formål med dem er opfyldt. Bilag II indeholder en liste over de dynamiske underfora, der skal etableres ved oprettelsen af informations- og varslingsnetværket.

### *Artikel 5 Medlemsstaternes rolle*

- 1) De deltagende medlemsstater udpeger en CIWIN-repræsentant og giver Kommissionen meddelelse herom. CIWIN-repræsentanten er ansvarlig for at give eller nægte at give adgangsrettigheder til informations- og varslingsnetværket i den pågældende medlemsstat.

- 2) De deltagende medlemsstater giver adgang til informations- og varslingsnetværket i overensstemmelse med de retningslinjer, Kommissionen har vedtaget.
- 3) De deltagende medlemsstater fremlægger og ajourfører regelmæssigt relevante oplysninger om beskyttelse af kritisk infrastruktur, der er af fælles interesse i EU.

#### *Artikel 6* *Kommissionens rolle*

- 1) Kommissionen har ansvaret for:
  - a) den tekniske udvikling og forvaltningen af informations- og varslingsnetværket, herunder dets it-struktur og elementerne til informationsudveksling
  - b) at fastsætte retningslinjer for betingelserne for anvendelsen af systemet, herunder fortrolighed, overførsel, lagring, arkivering og sletning af oplysninger. Kommissionen fastsætter betingelserne og procedurerne for at give fuld eller selektiv adgang til informations- og varslingsnetværket.
- 2) Kommissionen udpeger en CIWIN-repræsentant, der er ansvarlig for at give eller nægte at give adgangsrettigheder til informations- og varslingsnetværket i Kommissionen.
- 3) Kommissionen fremlægger og ajourfører regelmæssigt relevante oplysninger om beskyttelse af kritisk infrastruktur, der er af fælles interesse i EU.

#### *Artikel 7* *Sikkerhed*

- 1) Informations- og varslingsnetværket oprettes som et sikkert klassificeret system og skal være i stand til at behandle oplysninger op til niveauet "RESTREINT UE".

Kommissionen træffer beslutning om den mest hensigtsmæssige teknologiske platform for informations- og varslingsnetværket, og brugerne skal opfylde alle de tekniske krav, Kommissionen har fastsat.

Informations- og varslingsnetværkets sikkerhedsklassificering opgraderes efter behov.

- 2) Brugernes ret til at få adgang til dokumenter baseres på "behov for viden"-princippet og skal altid respektere ophavsmandens specifikke instrukser vedrørende beskyttelse og distribution af et dokument.
- 3) Medlemsstaterne og Kommissionen træffer de nødvendige sikkerhedsmæssige foranstaltninger for at:
  - a) forhindre uautoriserede personer i at få adgang til informations- og varslingsnetværket

- b) sikre, at autoriserede personer ved brug af informations- og varslingsnetværket kun har adgang til de data, der ligger inden for deres kompetenceområde
  - c) forhindre, at oplysninger i systemet bliver læst, kopieret, ændret eller slettet af uautoriserede personer.
- 4) Uploading af oplysninger til informations- og varslingsnetværket påvirker ikke ophavsretten til de pågældende oplysninger. De autoriserede brugere er alene ansvarlige for de oplysninger, de indlæser, og skal derfor sikre, at indholdet af disse fuldt ud er i overensstemmelse med gældende fællesskabsret og national ret.

*Artikel 8*  
*Retningslinjer for brugerne*

Kommissionen udvikler og ajourfører regelmæssigt retningslinjerne for brugerne, der indeholder alle detaljer om informations- og varslingsnetværkets funktioner og roller.

*Artikel 9*  
*Udgifter*

Udgifterne til driften og vedligeholdelsen af informations- og varslingsnetværket og dets centrale funktion dækkes over fællesskabsbudgettet. Udgifter vedrørende brugernes adgang til informations- og varslingsnetværket i de deltagende medlemsstater dækkes af de deltagende medlemsstater.

*Artikel 10*  
*Fornyelse vurdering*

Kommissionen tager driften af informations- og varslingsnetværket op til fornyet vurdering og evaluering hvert tredje år og fremlægger regelmæssige rapporter til medlemsstaterne.

Af den første rapport, der skal fremlægges senest tre år efter denne beslutnings ikrafttræden, skal det navnlig fremgå, hvilke af fællesskabsnetværkets elementer der bør forbedres eller tilpasses. Rapporten skal ligeledes indeholde forslag til ændringer eller tilpasninger af denne beslutning, som Kommissionen skønner nødvendige.

*Artikel 11*  
*Anvendelsesdato*

Denne beslutning finder anvendelse fra 1. januar 2009.

*Artikel 12  
Adressater*

Denne beslutning er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den.

*På Rådets vegne*

*Formand*

## **BILAG I**

### **PERMANENTE CIWIN-UNDERFORA**

De permanente underfora, der er omhandlet i artikel 4, omfatter følgende:

- 1) Medlemsstaternes underfora, der giver hver deltagende medlemsstat mulighed for at oprette sit eget forum inden for CIWIN-portalen. Organisationen, forvaltningen og indholdet af dette underforum vil alene være medlemsstaternes ansvar. Underforummet vil udelukkende være tilgængeligt for brugere fra den pågældende medlemsstat.
- 2) Sektorunderfora med 11 særskilte sektorer: kemisk industri, energi, finanssektoren, fødevarer, sundhedsvæsenet, informations- og kommunikationsteknologi, industrien i forbindelse med det nukleare brændselskredsløb, forskningsfaciliteter, rumfart, transport og vand. Der vil også være et tværsektorielt underforum med generiske emner og problemer af relevans for flere sektorer.
- 3) CIWIN-repræsentantens underforum, der tjener som platform for den strategiske koordination og samarbejdet med henblik på at fremme og øge arbejdet og kommunikationen for så vidt angår beskyttelse af kritisk infrastruktur. Kun CIWIN-repræsentanter vil have adgang til dette underforum.
- 4) Underforum for EU's samarbejde med tredjelande, hvor der fokuseres på at skabe bevidsthed om samarbejdet med tredjelande inden for beskyttelse af kritisk infrastruktur og standarder for denne type infrastruktur uden for EU.
- 5) Kontaktoversigt, der skal gøre det lettere at lede efter kontaktoplysninger om andre brugere af informations- og varslingsnetværket eller eksperter inden for beskyttelse af kritisk infrastruktur.

## **BILAG II**

### **DYNAMISKE CIWIN-UNDERFORA**

De dynamiske underfora, der er omhandlet i artikel 4, omfatter følgende:

- 1) Underforummet for arbejdsgruppen af eksperter, der skal understøtte arbejdet i ekspertgrupperne vedrørende beskyttelse af kritisk infrastruktur.
- 2) Projektunderforummet, der indeholder oplysninger om projekter, Kommissionen har finansieret.
- 3) Varslingsunderfora, der kan oprettes i tilfælde af en varslings i systemet for hurtig varslings, og som vil udgøre en kommunikationskanal i forbindelse med aktiviteter i tilknytning til beskyttelse af kritisk infrastruktur.
- 4) Underforum for særlige emner, hvor der sættes fokus på specifikke emner.

## FINANSIERINGSOVERSIGT TIL FORSLAGET

### 1. FORSLAGETS BETEGNELSE:

Rådets beslutning om et informations- og varslingsnetværk vedrørende kritisk infrastruktur (CIWIN)

### 2. ABM-/ABB-RAMME

Aktivitet 18.05: Sikkerhed og sikring af friheder

Mål nr. 2: Beskyttelse af kritisk infrastruktur

### 3. BUDGETPOSTER

#### 3.1. Budgetposternes nummer og tekst (aktionsposter og dermed forbundne poster vedrørende teknisk og administrativ bistand (tidl. B..A-poster)):

Budgetpost: 18.050800

Udgiftsområde: Forebyggelse, beredskab og konsekvensstyring i forbindelse med terrorisme.

#### 3.2. Foranstaltningens og de finansielle virkningers varighed:

Fra 2009 og fremefter

#### 3.3. Budgetoplysninger:

Budgetpost	Udgifternes art		Nye	EFTA-bidrag	Bidrag fra ansøgerlande	Udgiftsområde i de finansielle overslag
18.050800	Ikke-oblig.	Opdelte <sub>5</sub>	Nej	Nej	Nej	3A

---

<sup>5</sup> Opdelte bevillinger.

#### 4. SAMMENFATNING AF RESSOURCERNE

##### 4.1. Finansielle ressourcer

##### 4.1.1. Sammenfatning af forpligtelsesbevillinger (FB) og betalingsbevillinger (BB)

i mio. EUR (tre decimaler)

Udgiftstype	Punkt		2009	2010	2011	2012	2013	I alt
-------------	-------	--	------	------	------	------	------	-------

##### Driftsudgifter<sup>6</sup>

Forpligtelsesbevillinger (FB)	8.1.	a	0,95	0,55	0,55	0,55	0,55	3,15
Betalingsbevillinger (BB)		b	0,95	0,55	0,55	0,55	0,55	3,15

##### Administrative udgifter inden for referencebeløbet<sup>7</sup>

Teknisk og administrativ bistand (IOB)	8.2.4.	c	-	-	-	-	-	-
----------------------------------------	--------	---	---	---	---	---	---	---

##### SAMLET REFERENCEBELØB

<b>Forpligtelsesbevillinger</b>		a+c	0,95	0,55	0,55	0,55	0,55	3,15
<b>Betalingsbevillinger</b>		b+c	0,95	0,55	0,55	0,55	0,55	3,15

##### Administrative udgifter, der ikke er medtaget i referencebeløbet<sup>8</sup>

Personaleressourcer og dermed forbundne udgifter (IOB)	8.2.5.	d	0,117	0,117	0,117	0,117	0,117	0,585
Administrative udgifter, undtagen udgifter til personaleressourcer og dermed forbundne udgifter, ikke medtaget i referencebeløbet (IOB)	8.2.6.	e	0,015	0,015	0,015	0,015	0,015	0,075
<b>FB I ALT, inkl. udgifter til personaleressourcer</b>		a+c +d +e	1,082	0,682	0,682	0,682	0,682	3,81
<b>BB I ALT, inkl. udgifter til personaleressourcer</b>		b+c +d +e	1,082	0,682	0,682	0,682	0,682	3,81

<sup>6</sup> Udgifter, som ikke henhører under kapitel xx 01 i afsnit xx.

<sup>7</sup> Udgifter inden for artikel xx 01 04 i afsnit xx.

<sup>8</sup> Udgifter inden for kapitel xx 01, som ikke henhører under artikel xx 01 04 eller xx 01 05.

#### 4.1.2. Forenelighed med den finansielle programmering

- Forslaget er foreneligt med den gældende finansielle programmering.
- Forslaget kræver omprogrammering af det relevante udgiftsområde i de finansielle overslag.
- Forslaget kan kræve anvendelse af bestemmelserne i denne interinstitutionelle aftale<sup>9</sup> (dvs. fleksibilitetsinstrumentet eller revision af de finansielle overslag).

#### 4.1.3. Finansielle virkninger på indtægtssiden

- Forslaget har ingen indflydelse på indtægterne
- Forslaget har finansielle virkninger - virkningerne for indtægterne er som følger:

#### 4.2. Personaleressourcer (fuldtidsækvivalenter) (herunder tjenestemænd, midlertidigt ansatte og eksternt personale) - se nærmere under punkt 8.2.1.

Årligt behov	2009	2010	2011	2012	2013
Personaleressourcer i alt	1	1	1	1	1

### 5. SÆRLIGE FORHOLD OG MÅL

#### 5.1. Behov, der skal dækkes på kort eller lang sigt

Det særlige formål med informations- og varslingsnetværket er at gøre det muligt at sikre en koordinering og et samarbejde, hvad angår oplysninger om beskyttelse af kritisk infrastruktur på EU-plan. Det vigtigste er, at det bør garantere en sikker og struktureret udveksling af oplysninger og derved sætte brugerne i stand til at få viden om bedste praksis i andre EU-medlemsstater på en hurtig og effektiv måde og sætte medlemsstaterne i stand til at bruge systemet for hurtig varsling i forbindelse med beskyttelse af kritisk infrastruktur.

#### 5.2. Merværdien af Fællesskabets engagement og forslagens sammenhæng med andre finansielle instrumenter og eventuel synergi

Selv om det er hver enkelt medlemsstats ansvar at beskytte kritisk infrastruktur under dens jurisdiktion, kan en platform til udveksling af oplysninger, der dækker hele EU på tværs af grænserne, og som sikrer, at der står oplysninger til rådighed for alle medlemsstater, der kan have gavn heraf, kun gennemføres på EU-plan. Ingen medlemsstat alene kan sikre en udveksling af oplysninger eller en hurtig udveksling af varslinger på tværs af EU. Det er derfor tydeligt, at det giver en merværdi at arbejde på EU-plan for at koordinere de oplysninger, der allerede kan foreligge, men som ikke deles med andre. Kun en indsats på EU-plan kan sikre, at medlemsstater, der ønsker at dele og modtage oplysninger, behandles ens, at samarbejdet ikke virker diskriminerende rent geografisk for nogle medlemsstater, og at oplysningerne virkelig når frem til dem, der ønsker at modtage dem.

<sup>9</sup> Se punkt 19 og 24 i den interinstitutionelle aftale.

### 5.3. Forslagets mål, forventede resultater og øvrige indikatorer set i forbindelse med ABM-rammen

Informations- og varslingsnetværkets specifikke mål er at fremme udviklingen af hensigtsmæssige foranstaltninger med henblik på at lette udvekslingen af bedste praksis samt udgøre et værktøj til videreformidling af umiddelbare trusler og varslinger på sikker vis. Systemet bør sikre, at de rette personer får de rette oplysninger i rette øjeblik.

Oprettelsen af informations- og varslingsnetværket var allerede planlagt i meddelelsen om et europæisk program for beskyttelse af kritisk infrastruktur, og systemet selv som et it-redskab udgør et af EPCIP-programmets operationelle mål. Det operationelle (under)mål, det er hensigten at nå ved hjælp af informations- og varslingsnetværket, kan indkredses som følger:

- at tilvejebringe et it-redskab, der letter samarbejdet om beskyttelse af kritisk infrastruktur mellem medlemsstaterne, der udgør et effektivt og hurtigt alternativ til tidskrævende metoder til at søge efter oplysninger om kritisk infrastruktur i Fællesskabet, og som vil give medlemsstaterne mulighed for at kommunikere direkte og uploade de oplysninger, de skønner er relevante.

### 5.4. Gennemførelsesmetode (vejledende)

- Central forvaltning**
  - Direkte af Kommissionen
  - Indirekte ved delegation til:
    - Forvaltningsorganer
    - Organer oprettet af Fællesskaberne, jf. artikel 185 i finansforordningen
    - Nationale offentlige organer eller public service-organer
- Fælles eller decentral forvaltning**
  - med medlemsstaterne
  - med tredjelande
- Fælles forvaltning med internationale organisationer (angiv nærmere)**

Relevante bemærkninger:

## **6. OVERVÅGNING OG EVALUERING**

### **6.1. Overvågningssystem**

Følgende indikatorer til at vurdere de fremskridt, der gøres, vil blive anvendt i forbindelse med informations- og varslingsnetværket.

- Antallet af medlemsstater, der deltager i informations- og varslingsnetværket (mindst 20 medlemsstater bør anvende det regelmæssigt, for at det kan blive en succes).
- Graden af fortrolighed af de oplysninger, der udveksles (uploader medlemsstaterne kun ikke-klassificerede oplysninger, eller uploades der også klassificerede oplysninger?).
- Bruger eksperterne inden for beskyttelse af kritisk infrastruktur også informations- og varslingsnetværket som et hovedredskab til at udveksle meninger for at nå deres mål (f.eks. fastlæggelse af kriterierne for at indkredse kritisk infrastruktur i specifikke sektorer)?

### **6.2. Evaluering**

#### *6.2.1. Forudgående evaluering*

Efter afslutningen af testperioden (CIWIN-pilotprojektet) i 2009 vil Kommissionen sende et kort spørgeskema til medlemsstaternes myndigheder for at vurdere deres tilfredshed med systemet og kontrollere, om det bidrager til de generelle mål for CIWIN-initiativet (og forslag til mulige nye funktioner eller fjernelse af funktioner, der ikke fungerer så godt).

Der er desuden gennemført en konsekvensanalyse, der er knyttet til dette forslag.

#### *6.2.2. Forholdsregler efter en midtvejsevaluering eller efterfølgende evaluering (konklusioner, der kan drages af lignende tidligere erfaringer)*

Den væsentligste ordning for overvågning og evaluering bør fokusere på princippet om "kundetilfredshed".

- Kommissionen bør tage det funktionelle system op til fornyet vurdering hvert tredje år. Kommissionen skal basere sin revision på medlemsstaternes holdninger, der indhentes på regelmæssige møder for kontaktpunkterne for beskyttelse af kritisk infrastruktur.

#### *6.2.3. Regler for fremtidige evalueringer og deres hyppighed*

Informations- og varslingsnetværket skal vurderes i lyset af de indikatorer, der er nævnt under 6.1., tre år efter, at det blev oprettet.

## **7. FORHOLDSREGLER MOD SVIG**

Beskyttelse af Fællesskabets finansielle interesser og bekæmpelse af svig og uregelmæssigheder udgør en integrerende del af denne beslutning.

Det er den relevante tjeneste i Kommissionen, der har ansvaret for den administrative overvågning af kontrakter og betalinger. De relevante tjenester i Kommissionen vil føre tilsyn med hver af de foranstaltninger, der finansieres i medfør af denne beslutning, i alle faser af

projektet. I forbindelse med tilsynet tages der hensyn til de kontraktmæssige forpligtelser og principperne om analyse af omkostningseffektiviteten og en sund finansforvaltning.

Derudover vil der i enhver aftale eller kontrakt, der indgås i medfør af denne beslutning, udtrykkeligt, blive fastsat bestemmelse om, at Kommissionen vil føre tilsyn med anvendelsen af midlerne inden for rammerne af projekterne/programmerne, og at aktiviteterne gennemføres efter hensigten. Kommissionen og Det Europæiske Kontor for Bekæmpelse af Svig (OLAF) vil desuden føre finansiel kontrol, og Revisionsretten vil foretage revisioner, om nødvendigt i marken. Det skal i henhold til aftalerne eller kontrakterne være muligt for Kommissionen (OLAF) at foretage kontrol og inspektion på stedet i overensstemmelse med Rådets forordning (EF) nr. 2185/96 af 11. november 1996 om Kommissionens kontrol og inspektion på stedet med henblik på beskyttelse af De Europæiske Fællesskabers finansielle interesser mod svig og uregelmæssigheder.

Der vil blive lagt særlig vægt på udgifternes art (udgifternes støtteberettigelse), overholdelsen af budgetterne (faktiske udgifter) og kontrol af støtteoplysninger og relevant dokumentation (bilag for udgifter).

## 8. RESSOURCER

### 8.1. Finansielle omkostninger i forbindelse med forslaget mål

Forpligtelsesbevillinger i mio. EUR (tre decimaler)

(Beskrivelse af mål, foranstaltninger og output)	Type output	Gen. snit. omkostn.	2009		2010		2011		2012		2013		I ALT	
			Antal output	Samlede omkostninger	Antal output	Samlede omkostninger	Antal output	Samlede omkostninger	Antal output	Samlede omkostninger	Antal output	Samlede omkostninger	Antal output	Samlede omkostninger
OPERATIONELT MÅL nr. 1 <sup>10</sup> : at tilvejebringe et it-redskab, der vil lette samarbejdet om beskyttelsen af kritisk infrastruktur mellem medlemsstaterne														
Foranstaltning: At oprette og forvalte et system til hurtig varsling vedrørende beskyttelse af kritisk infrastruktur og oprette et forum for udveksling af bedste praksis														

<sup>10</sup> Som beskrevet i afsnit 5.3.

(Beskrivelse af mål, foranstaltninger og output)	Type output	Gen. snit. omkostn.	2009		2010		2011		2012		2013		I ALT	
			Antal output	Samlede omkostninger	Antal output	Samlede omkostninger	Antal output	Samlede omkostninger	Antal output	Samlede omkostninger	Antal output	Samlede omkostninger	Antal output	Samlede omkostninger
Output 1	Vært for funktionen hurtig varsling i forbindelse med informations- og varslingsnetværket (sikkert miljø)	0,3	1	0,3	1	0,3	1	0,3	1	0,3	1	0,3	5	1,5
- Output 2	Support og vedligeholdelse af systemet	0,25	1	0,25	1	0,25	1	0,25	1	0,25	1	0,25	5	1,25
- Output 3	Den nødvendige tekniske support til sikkerhedsakkreditering, vedligeholdelse, oprettelse af en helpdesk og uddannelseskuser	0,07	1	0,4									1	0,4
<b>SAMLEDE OMKOSTNINGER</b>		0,617	1	0,95	1	0,55	1	0,55	1	0,55	1	0,55	5	3,15

## 8.2. Administrative udgifter

### 8.2.1. Personaleressourcer – antal og type

Stillingstyper	Personale til forvaltning af foranstaltningen ved brug af eksisterende og/eller yderligere ressourcer ( <b>antal stillinger/fuldtidsækvivalenter</b> )											
			2009	2010	2011	2012	2013					
(18)	(20)	AD	(21)	0,5	(22)	0,5	(23)	0,5	(24)	0,5	(25)	0,5
(19)		AST		0,5		0,5		0,5		0,5		0,5
Tjenestemænd eller midlertidigt ansatte <sup>11</sup>												
(XX 01 01)												
Personale, der finansieres <sup>12</sup> over art. XX 01 02												
Andet personale, der finansieres <sup>13</sup> over art. XX 01 04/05												
<b>I ALT</b>			<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>1</b>				

### 8.2.2. Opgavebeskrivelse

Hovedopgaven for Kommissionens tjenestemænd vil være at udføre CIWIN-administratorers opgaver. De vil derfor være ansvarlige for konfigurationen af denne løsning, forvalte anmodninger om oprettelse af dynamiske underfora og være ansvarlige for oprettelsen af dynamiske underfora og fjernelsen af underfora, der ikke bruges eller er opgivet. Kommissionen får rollen som administrator.

### 8.2.3. Kilde til personaleressourcer (vedtægtsomfattede)

- Stillinger, der i øjeblikket er afsat til forvaltningen af programmet, og som skal erstattes eller forlænges
- Stillinger, der er forhåndsallokeret i forbindelse med APS/FBF-proceduren for år n

<sup>11</sup> Cost of which is NOT covered by the reference amount

<sup>12</sup> Udgifter, der IKKE er medtaget i referencebeløbet.

<sup>13</sup> Udgifter, der er medtaget i referencebeløbet.

- Stillinger, hvorom der skal ansøges i forbindelse med den næste APS/FBF-procedure
- Stillinger, som skal omfordeles under anvendelse af eksisterende ressourcer inden for den pågældende tjeneste (intern omfordeling)
- Stillinger, der er nødvendige i år n, men ikke forudset i APS/FBF-proceduren for det pågældende år

8.2.4. *Andre administrative udgifter, der er medtaget i referencebeløbet (XX 01 04/05 - udgifter til administrativ forvaltning)*

i mio. EUR (tre decimaler)

Budgetpost (nummer og betegnelse)	2009	2010	2011	2012	2013	I ALT
<b>1 Teknisk og administrativ bistand (herunder personaleudgifter)</b>						
Forvaltningsorganer <sup>14</sup>	-	-	-	-	-	-
Anden teknisk og administrativ bistand	-	-	-	-	-	-
- intern						
- ekstern						
<b>Teknisk og administrativ bistand i alt</b>	-	-	-	-	-	-

8.2.5. *Udgifter til personaleressourcer og dermed forbundne udgifter, der ikke er medtaget i referencebeløbet*

i mio. EUR (tre decimaler)

Arten af personaleressourcer	2009	2010	2011	2012	2013
Tjenestemænd og midlertidigt ansatte (XX 01 01)	0,117	0,117	0,117	0,117	0,117
Personale finansieret over artikel XX 01 02 (hjelpeansatte, nationale eksperter, kontraktansatte osv.)  (oplys budgetpost)					

<sup>14</sup> Der skal henvises til den specifikke finansieringsoversigt for det eller de pågældende forvaltningsorganer.

<b>Samlede udgifter til personaleressourcer og dermed forbundne udgifter (IKKE medtaget i referencebeløbet)</b>	0,117	0,117	0,117	0,117	0,117
-----------------------------------------------------------------------------------------------------------------	-------	-------	-------	-------	-------

Beregning - *tjenestemænd og midlertidigt ansatte*

Se punkt 8.2.1.

Beregning - *personale, der finansieres over art. XX 01 02*

Ikke relevant.

	2009	2010	2011	2012	2013	I ALT
XX 01 02 11 01 — Tjenesterejser	0,01	0,01	0,01	0,01	0,01	0,05
XX 01 02 11 02 – Møder og konferencer	0,005	0,005	0,005	0,005	0,005	0,025
XX 01 02 11 03 — Udvalg <sup>15</sup>	-	-	-	-	-	-
XX 01 02 11 04 – Undersøgelser og høringer	-	-	-	-	-	-
XX 01 02 11 05 - Informationssystemer	-	-	-	-	-	-
<b>2 Andre forvaltningsudgifter i alt (XX 01 02 11)</b>	-	-	-	-	-	-
<b>3 Andre udgifter af administrativ karakter (angiv hvilke, herunder budgetpost)</b>	-	-	-	-	-	-
<b>Administrative udgifter i alt, undtagen udgifter til personaleressourcer og dermed forbundne udgifter (IKKE medtaget i referencebeløbet)</b>	0,015	0,015	0,015	0,015	0,015	0,075

Beregning - *Andre administrative udgifter, der ikke er medtaget i referencebeløbet*

Ikke relevant.

<sup>15</sup> Oplys, hvilken type udvalg det drejer sig om, og hvilken gruppe det tilhører.