EUROPEISKA KOMMISSIONEN

Bryssel den 30.9.2010
KOM(2010) 521 slutlig

2010/0275 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om Europeiska byrån för nät- och informationssäkerhet (Enisa)

{SEK(2010) 1126}
{SEK(2010) 1127}

MOTIVERING

1. BAKGRUND

1.1. Politiskt sammanhang

Genom förordning (EG) nr 460/2004[1] inrättades Europeiska byrån för nät- och informationssäkerhet (Enisa) i mars 2004 för en inledande period på fem år med huvudmålet att *”säkerställa en hög nivå på nät- och informationssäkerhet i gemenskapen och utveckla en kultur av nät- och informationssäkerhet till förmån för medborgarna, konsumenterna, företagen och den offentliga sektorns organisationer i Europeiska unionen och på det sättet bidra till att den inre marknaden fungerar väl”*. Genom förordning 1007/2008[2] förlängdes Enisas mandat till mars 2012.

När Enisas mandat förlängdes 2008 inleddes också en debatt om den allmänna inriktningen på EU:s arbete för nät- och informationssäkerhet, till vilken kommissionen bidrog genom att ta initiativ till ett offentligt samråd om de tänkbara målen för en stärkt nät- och informationssäkerhetspolitik på EU-nivå. Detta offentliga samråd pågick från november 2008 till januari 2009 och nästan 600 bidrag kom in[3].

Den 30 mars 2009 antog kommissionen ett meddelande om skydd av kritisk informationsinfrastruktur[4], *Skydd mot storskaliga it-attacker och avbrott: förbättrad beredskap, säkerhet och motståndskraft i Europa*, med en handlingsplan där byrån uppmanas att vara aktiv, framför allt för att stödja medlemsstaterna. Handlingsplanen fick ett brett stöd i de diskussioner som fördes vid ministerkonferensen om skydd av kritisk infrastruktur i Tallinn i Estland den 27 och 28 april 2009[5]. I slutsatserna från EU-ordförandeskapets konferens betonas att det är viktigt att *se till att Enisas verksamhet får ett ordentligt stöd*. Vidare konstateras att Enisa *är ett utmärkt instrument för att främja ett EU-täckande samarbete inom detta område* och poängterar att byråns mandat bör ses över och omformuleras *för att i ökad utsträckning inrikta sig på EU:s prioriteringar och behov, klara att reagera på händelser på ett mer flexibelt sätt, utveckla förmågor och kompetenser och öka byråns operativa effektivitet och övergripande inflytande* för att göra den till en *ständig tillgång för varje medlemsstat och hela Europeiska unionen.*

Efter diskussionerna i rådet (telekommunikation) den 11 juni 2009 där medlemsstaterna uttryckte sitt stöd för att förlänga byråns mandat och ge den mer resurser, mot bakgrund av nät- och informationssäkerhetens betydelse och de nya utmaningarna inom det här området, slutfördes diskussionen under det svenska ordförandeskapet. I rådets resolution av den 18

---

1 Europaparlamentets och rådets förordning (EG) nr 460/2004 av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet, EUT L 77, 13.3.2004, s. 1.

2 Europaparlamentets och rådets förordning (EG) nr 1007/2008 av den 24 september 2008 om ändring av förordning (EG) nr 460/2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet i fråga om dess mandatperiod, EUT L 293, 31.10.2008, s.1.

3 Rapporten som sammanfattar resultaten från det offentliga samrådet, *Towards a Strengthened Network and Information Security Policy in Europe*, bifogas som bilaga 11 till konsekvensanalysen för detta förslag.

4 KOM(2009) 149, 30.3.2009.

5 Diskussionsdokument: http://www.tallinnciip.eu/doc/discussion_paper_-_tallinn_ciip_conference.pdf Ordförandeskapets slutsatser: http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf.

december 2009 om en europeisk samarbetsstrategi för nät- och informationssäkerhet[6] erkänns byråns betydelse och potential samt behovet av att *”utveckla Enisa vidare till ett effektivt organ.”* Där betonas också att byrån måste moderniseras och stärkas för att stödja kommissionen och medlemsstaterna i arbetet med att överbrygga klyftan mellan teknik och politik och fungera som EU:s kunskapscentrum i frågor som rör nät- och informationssäkerhet.

1.2. Allmän bakgrund

Informations- och kommunikationsteknik har blivit en hörnsten i EU:s ekonomi och för samhället som helhet. Informations och kommunikationstekniken är sårbar för hot som inte längre följer nationella gränser och som har förändrats i takt med teknikens och marknadens utveckling. Eftersom informations- och kommunikationstekniken är global, sammankopplad och beroende av annan infrastruktur kan säkerhet och motståndskraft inte uppnås med enbart nationella och okoordinerade metoder. Dessutom förändras nät- och informationssäkerhetsproblemen snabbt. Näten och informationssystemen måste skyddas effektivt mot alla typer av störningar och avbrott, även avsiktliga angrepp.

Politiken för nät- och informationssäkerhet har en viktig plats i den digitala agendan för Europa[7], som är ett centralt initiativ inom strategin Europa 2020, som syftar till att utnyttja och främja informations- och kommunikationsteknikens potential och omvandla denna potential till hållbar tillväxt och innovation. Några centrala prioriteringar för initiativet är att främja IKT-användning och bygga upp förtroendet för informationssamhället.

Enisa inrättades ursprungligen för säkra en hög och effektiv nivå på nät- och informationssäkerheten i EU. Erfarenheterna från byråns arbete och utmaningarna och hoten har gjort det uppenbart att byråns mandat måste moderniseras till att bättre fylla EU:s behov när det gäller sådant som

- fragmenteringen av de nationella strategierna för att hantera de föränderliga utmaningarna,
- bristen på samverkansmodeller för genomförandet av nät- och informationssäkerhetspolitiken,
- den otillräckliga beredskapen som också beror på den begränsade europeiska kapaciteten för tidig varning och reaktion,
- bristen på tillförlitliga EU-data och de begränsade kunskaperna om föränderliga problem,
- den låga graden av medvetenhet om risker och utmaningar förknippade med nät- och informationssäkerhet, och
- utmaningen att integrera nät- och informationssäkerhetsaspekter i politiska strategier för att bekämpa nätbrottslighet på ett effektivare sätt.

---

6 Rådets resolution av 18 december 2009 om en europeisk samarbetsstrategi för nät- och informationssäkerhet, EUT C 321, 29.12.2009, s. 1. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF.

7 KOM(2010) 245, 19.5.2010.

1.3. Politiska mål

Det allmänna målet för den föreslagna förordningen är att göra det möjligt för EU, medlemsstaterna och aktörerna att utveckla en hög kapacitet och beredskap för att förebygga, spåra och bättre reagera på nät- och informationssäkerhetsproblem. Detta kommer att bidra till att bygga upp ett förtroende som främjar utvecklingen av informationssamhället, för att förbättra konkurrenskraften för europeiska företag och säkerställa en effektivt fungerande inre marknad.

1.4. Gällande bestämmelser

Det här förslaget kompletterar andra lagstiftningsinitiativ och politiska initiativ inom området nät- och informationssäkerhet på EU-nivå som syftar till att förbättra informations- och kommunikationsteknikens säkerhet och motståndskraft.

- Den handlingsplan som lanserades genom meddelande om skydd av kritisk informationsinfrastruktur omfattade inrättandet av både

  (1) ett EU-forum för medlemsstaterna som ska främja diskussion och utbyte av god praxis syftande till gemensamma politiska mål och prioriteringar för IKT-infrastrukturens säkerhet och motståndskraft, vilket också direkt gagnas av det arbete och stöd som byrån kan ge, och

  (2) ett offentligprivat EU-partnerskap för motståndskraft (EP3R), som är en flexibel europeisk ram för IKT-infrastrukturens motståndskraft. Partnerskapet ska främja samarbete mellan offentlig och privat sektor i säkerhets- och motståndskraftsfrågor, grundläggande krav, god policy och åtgärder.

- Stockholmsprogrammet, som antogs av Europeiska rådet den 11 december 2009, främjar strategier för att garantera nätsäkerhet och möjliggöra snabbare reaktioner vid it-attacker i EU.

- Dessa initiativ bidrar till genomförandet av den digitala agendan för Europa. Politiken för nät- och informationssäkerhet har stor betydelse för den del av strategin som inriktas på att bygga upp förtroendet och säkerheten i informationssamhället. Initiativen understödjer också kommissionens stödåtgärder och politik för skydd av personlig integritet (t.ex. inbyggda skyddsmekanismer för den personliga integriteten) och personuppgifter (översyn av ramen), nätverket för konsumentskyddssamarbetet och programmet för ett säkrare Internet.

1.5. Utveckling inom den nuvarande nät- och informationssäkerhetspolitiken kopplad till förslaget

Mycket av den nuvarande utvecklingen av nät- och informationssäkerhetspolitiken, i synnerhet den som aviserades i den digitala agendan för Europa, gagnas av det stöd och de expertkunskaper som byrån kan tillhandahålla. Några exempel är följande:

- Stärka samarbetet om nät- och informationssäkerhetsfrågor genom intensifierad verksamhet i **EU-forumet för medlemsstater (EFMS)**, som med direkt stöd från byrån kommer att bidra till att

– fastställa hur ett effektivt europeiskt nät ska kunna inrättas genom gränsöverskridande samarbete mellan nationella och statliga incidenthanteringsorganisationer (Computer Emergency Response Team, CERT),

– fastställa långsiktiga mål och prioriteringar för storskaliga europeiska övningar om nät- och informationssäkerhetsincidenter,

– verka för minimikrav i offentlig upphandling för att främja säkerhet och motståndskraft i offentliga system och nät,

– hitta ekonomiska och rättsliga incitament för säkerhet och motståndskraft, och

– utvärdera nät- och informationssäkerhetsläget i Europa.

- Stärka samarbeten och partnerskap mellan offentlig och privat sektor genom att stödja **det offentligprivata EU-partnerskapet för motståndskraft (EP3R)**. Enisa får en alltmer framträdande roll som främjare av EP3R-möten och –verksamheter. EP3R närmaste åtgärder kommer att omfatta följande:

  – diskussion av innovativa åtgärder och instrument som ska förbättra säkerheten och motståndskraften, som t.ex.

  (1) grundläggande krav när det gäller säkerhet och motståndskraft, i synnerhet i samband med offentlig upphandling av IKT-produkter eller tjänster, för att ge alla samma konkurrensvillkor och samtidigt säkra en lämplig nivå på beredskap och förebyggande åtgärder,

  (2) diskussion kring frågor som rör ekonomiska aktörers ansvar, när de t.ex. inför minimisäkerhetskrav,

  (3) ekonomiska incitament för utveckling och tillämpning av riskhanteringsmetoder, säkerhetsprocesser och säkerhetsprodukter,

  (4) riskbedömnings och riskhanteringssystem för att bedöma och hantera allvarliga incidenter på grundval av gemensam förståelse,

  (5) samarbete mellan offentlig och privat sektor i samband med storskaliga incidenter, och

  (6) anordnande av ett **företagstoppmöte** om ekonomiska hinder och drivkrafter för säkerhet och motståndskraft.

- Praktiskt tillämpa säkerhetskraven i regelverket för elektronisk kommunikation, för vilket man behöver Enisas expertis och bistånd

  – för att stödja medlemsstaterna och kommissionen, om lämpligt med beaktande av privata sektorns synpunkter, vid fastställandet av en ram av regler och förfaranden för att genomföra bestämmelserna om anmälan av säkerhetsöverträdelser (enligt artikel 13.a i det ändrade ramdirektivet), och

  – för att inrätta ett årligt forum för nationella behöriga organ och nationella regleringsmyndigheter på området nät- och informationssäkerhet och aktörer från

privata sektorn, för att diskutera lärdomar som gjorts och utbyta god praxis för tillämpningen av regleringsåtgärder för nät- och informationssäkerhet.

- Främja **EU-täckande beredskapsövningar avseende it-säkerhet** med stöd av kommissionen och bidrag av Enisa. Tanken är att den här typen av övningar senare ska utvidgas på internationell nivå.

- **Inrätta en grupp för stöd vid datorhaveri (Cert) för EU:s institutioner.** Enligt nyckelåtgärd 6 i den digitala agendan för Europa ska kommissionen lägga fram ”åtgärder för en stärkt politik för nät- och informationssäkerhet på hög nivå, bl.a. […]åtgärder för att möjliggöra snabbare insatser vid cyberattacker, inklusive en incidenthanteringsorganisation för EU-institutionerna”[8]. Därför måste kommissionen och andra EU-institutioner göra en analys och inrätta en incidenthanteringsorganisation för vilken Enisa kan tillhandahålla tekniskt stöd och expertis.

- Mobilisera och stödja medlemsstaterna när det gäller att färdigställa och om nödvändigt inrätta **nationella/statliga incidenthanteringsorganisationer för att skapa ett välfungerande nätverk av sådana som täcker hela Europa**. Det här kommer också att vara viktigt för att vidareutveckla ett EU-system för informationsutbyte och varning (Eisas) för medborgare och små och medelstora företag som ska byggas upp med nationella resurser och kompetenser före utgången av 2012.

- **Öka medvetenheten** om nät- och säkerhetsutmaningar, vilket kommer att omfatta

  – att kommissionen tillsammans med Enisa utarbetar riktlinjer för främjandet av nät- och informationssäkerhetsstandarder, god praxis och en riskhanteringskultur; En första uppsättning riktlinjer kommer att sammanställas, och

  – att Enisa i samarbete med medlemsstaterna anordnar **”den europeiska månaden för nät- och informationssäkerhet för alla”**, med nationella/europeiska cybersäkerhetstävlingar.

1.6. Förenlighet med Europeiska unionens politik och mål på andra områden

Förslaget är förenligt med Europeiska unionens politik och mål och helt i enlighet med målet att bidra till en välfungerande inre marknad, genom ökad beredskap och reaktionsförmåga för utmaningar på området nät- och informationssäkerhet.

2. RESULTATEN AV DE OFFENTLIGA SAMRÅDEN OCH KONSEKVENSANALYSERNA

2.1. Samråd med berörda parter

Det här initiativet är resultatet av en omfattande diskussion med brett deltagande som förts i enlighet med principerna om deltagande, öppenhet, redovisningsskyldighet, effektivitet och samstämmighet. Den breda processen omfattade en utvärdering av Enisa under 2006/2007

[8] Rådets resolution av den 18 december 2009 om en europeisk samarbetsstrategi för nät- och informationssäkerhet: *Europeiska unionens råd […] som är medvetet om […] vikten av att man undersöker vilka strategiska effekter, risker och möjligheter som är förbundna med inrättande av CERT-organisationer för EU-institutionerna och överväger Enisas eventuella framtida roll i detta.*

följd av rekommendationer från byråns styrelse, två offentliga samråd (2007 och 2008–2009) samt ett antal seminarier om nät- och informationssäkerhetsfrågor.

Det första offentliga samrådet inleddes i samband med kommissionens meddelande om halvtidsutvärderingen av Enisa. Samrådet fokuserades på byråns framtid och löpte mellan den 13 juni och den 7 september 2007. Totalt inkom 44 onlinebidrag plus två andra skriftliga bidrag. Svaren kom från många olika typer av aktörer och berörda parter, som ministerier i medlemsstaterna, regleringsorgan, branschen, konsumentorganisationer, akademiska institutioner, företag och enskilda medborgare.

Svaren belyste flera intressanta frågor som rörde hotscenariots utveckling, behovet av att förtydliga och bygga in mer flexibilitet i förordningen så att Enisa kan anpassas till dessa utmaningar, behovet av effektiv interaktion med aktörerna och möjligheten till en begränsad ökning av resurserna.

Det andra offentliga samrådet, som löpte från den 7 november 2008 till den 9 januari 2009, syftade till att fastställa prioriterade mål för en stärkt nät- och informationssäkerhetspolitik på EU-nivå och hur dessa mål ska uppnås. Nästan 600 bidrag inkom från medlemsstaternas myndigheter, akademiska världen och forskningsinstitut, branschorganisationer, privata företag och andra aktörer, som dataskyddsorganisationer och konsulter, samt privatpersoner.

En stor majoritet av deltagarna[9] stödde en utvidgning av byråns mandat och förespråkade att den skulle få en mer framträdande roll i samordningen av nät- och informationssäkerhetsverksamhet på EU-nivå och tilldelas ökade resurser. De viktigaste prioriteringarna var ett mer samordnat agerande mot cyberhot i Europa, ett gränsöverskridande samarbete för hantering av storskaliga cyberattacker, satsningar på att bygga upp förtroendet och ett förbättrat utbyte av information mellan intressenter.

En konsekvensanalys gjordes av förslaget, med början i september 2009. Den grundades på en förberedande studie som utförts av en extern uppdragstagare. Många olika aktörer och experter deltog. Bidrag kom från bl.a. nät- och informationssäkerhetsorgan i medlemsstaterna, nationella regleringsmyndigheter, teleoperatörer och Internetleverantörer samt deras branschorganisationer, konsumentorganisationer, IKT-tillverkare, incidenthanteringsorganisationer, den akademiska världen och företagsanvändare. Man inrättade också en avdelningsöverskridande styrgrupp, bestående av företrädare för de berörda generaldirektoraten inom kommissionen, för att stödja arbetet med konsekvensanalysen.

2.2. Konsekvensanalys

Det fastställdes att bibehållandet av en byrå var en lämplig lösning för att uppnå EU:s mål inom området[10]. Efter en inledande genomgång valdes följande fem alternativ ut för vidare analys:

- Alternativ 1 — Ingen politik.
- Alternativ 2 — Oförändrade förhållanden, dvs. att fortsätta med ett liknande mandat och samma resursnivå.

[9] Se bilaga XI till konsekvensanalysen.
[10] Se bilaga IV till konsekvensanalysen.

- Alternativ 3 — Att utöka Enisas uppgifter och låta myndigheter som sysslar med brottsbekämpning och integritetsskydd bli fullvärdiga parter.

- Alternativ 4 — Att lägga bekämpande av cyberattacker och reaktion på cyberincidenter till byråns uppgifter.

- Alternativ 5 — Att utöka byråns uppgifter med stöd till ordningsmakt och rättsliga myndigheter i bekämpandet av cyberbrottslighet.

Efter en jämförande kostnads-nyttoanalys fastställdes alternativ 3 som det mest kostnadseffektiva och effektiva sättet att uppnå målen.

Alternativ 3 innebär att Enisas uppgifter utvidgas och fokuserar på

- att bygga upp och underhålla ett nätverk för kontakter mellan intressenter och ett kunskapsnät som säkerställer att Enisa har god överblick över nät- och informationssäkerheten i Europa,
- att fungera som ett stödcentrum för nät- och informationssäkerhet vid utformning och genomförande av politiska strategier (i synnerhet när det gäller e-integritet, e-signatur, e-legitimation och upphandlingsstandarder för nät- och informationssäkerhet),
- att stödja EU:s politik för skydd av kritisk informationsinfrastruktur och motståndskraft (t.ex. övningar, EP3R och EU-systemet för informationsutbyte och varning),
- att skapa en EU-ram för insamling av data om nät- och informationssäkerhet, inbegripet utveckling av metoder och praxis för laglig rapportering och förmedling av data,
- att studera nät- och informationssäkerhetens ekonomi,
- att främja samarbete med tredjeländer och internationella organisationer för att uppnå en gemensam global syn på nät- och informationssäkerhet och se till att internationella initiativ på hög nivå får genomslag i Europa, och
- utföra icke-operativa uppgifter kopplade till nät- och informationssäkerhetsaspekter av polisiärt arbete och rättsligt samarbete om cyberbrottslighet.

3. RÄTTSLIGA ASPEKTER

3.1. Sammanfattning av den föreslagna åtgärden

Förslaget till förordning syftar till att stärka och modernisera Europeiska byrån för nät- och informationssäkerhet (Enisa) och fastställa ett nytt mandat för en femårsperiod.

Förslaget omfattar följande viktiga förändringar jämfört med den ursprungliga förordningen:

(1) **Ökad flexibilitet, anpassningsbarhet och fokusering.** Uppgifterna uppdateras och ges en mer allmän formulering för att öka utrymmet för byråns verksamhet. Uppgifterna formuleras tillräckligt exakt för att beskriva hur målen ska uppnås. Det här ger ett starkare fokus åt byråns uppdrag, ökar dess förmåga att uppnå sina mål och stärker dess uppdrag för att stödja genomförandet av EU:s politik.

(2) **Bättre anpassning av byrån till EU:s politik och lagstiftningsprocess.** EU:s institutioner och organ kan vända sig till byrån för bistånd och rådgivning. Detta är i

linje med politikens och lagstiftningens utveckling. Rådet har börjat vända sig direkt till byrån i resolutioner, och Europaparlamentet och rådet har delegerat uppgifter som rör nät- och informationssäkerhet till byrån i regelverket för elektronisk kommunikation.

(3) **Kontaktyta mot bekämpandet av cyberbrottslighet.** I sitt arbete för att uppnå målen beaktar byrån kampen mot cyberbrottslighet. Rättsvårdande myndigheter och myndigheter som ansvarar för skydd av personlig integritet blir fullvärdiga intressenter i byrån, i synnerhet i den ständiga intressentgruppen.

(4) **Stärkta styrelseformer.** Föreslaget stärker tillsynsfunktionen för styrelsen, där medlemsstaterna och kommissionen är företrädda. Styrelsen kan t.ex. utfärda allmänna riktlinjer för personalfrågor, vilket tidigare helt tillhörde verkställande direktörens ansvarsområde. Den får också inrätta arbetsgrupper som kan bistå den i dess uppgifter, inbegripet övervakandet av hur dess beslut genomförs.

(5) **Förenklade förfaranden.** Förfaranden som har visat sig vara onödigt betungande förenklas. Exempel: a) Ett förenklat förfarande för styrelsens interna regler, b) yttrandet om Enisas arbetsprogram utfärdas av kommissionens avdelningar och inte genom ett kommissionsbeslut. Styrelsen ges också tillräckliga resurser för att kunna fatta och genomföra verkställande beslut (t.ex. om en personalmedlem inkommer med klagomål mot verkställande direktören eller mot själva styrelsen).

(6) **Gradvis ökning av resurser.** För att klara de stärkta europeiska kraven och de utvidgade utmaningarna kommer byråns finansiella resurser och personalresurser gradvis att ökas mellan 2012 och 2016, utan att det påverkar kommissionens förslag till nästa fleråriga budgetram. På grundval av kommissionens förslag till förordning om flerårig budgetram för perioden efter 2013 och med beaktande av slutsatserna från konsekvensanalysen, kommer kommissionen att lägga fram en ändrad finansieringsöversikt för rättsakt.

(7) **Möjlighet att förlänga verkställande direktörens mandatperiod.** Styrelsen får förlänga verkställande direktörens mandatperiod med tre år.

3.2. Rättslig grund

Förslaget baseras på artikel 114 i fördraget om Europeiska unionens funktionssätt (EU-fördraget)[11].

I enlighet med EG-domstolens dom[12] före Lissabonfördragets ikraftträdande ansågs **artikel 95 i EG-fördraget** vara den lämpliga rättsliga grunden för inrättandet av ett organ som ska säkra en hög och effektiv nivå av nät- och informationssäkerhet i EU. Genom att använda uttrycket ”åtgärder för tillnärmning” i artikel 95 avser fördragets författare att ge EU:s lagstiftare rätt att välja vilka åtgärder som är lämpliga för att uppnå det önskade resultatet. Att förbättra säkerheten och motståndskraften för IKT-infrastrukturer och motståndskraft är alltså en viktig aspekt som bidrar till en välfungerande inre marknad.

---

11 EUT C 115, 9.5.2008, s. 94.

12 Mål C-217/04, Förenade konungariket Storbritannien och Nordirland mot Europaparlamentet och Europeiska unionens råd, Reg. 2.5.2006.

I enlighet med Lissabonfördraget beskriver **artikel 114 i EU-fördraget**[13] inre ansvaret för inre marknaden nästan identiskt. Av de skäl som redan angetts kommer detta även i fortsättningen att vara den rättsliga grund som ska tillämpas vid antagandet av åtgärder för att förbättra nät- och informationssäkerheten. EU och medlemsstaterna har i dag delade befogenheter när det gäller inre marknaden (artikel 4.2 a i EU-fördraget). Detta betyder att EU och medlemsstaterna får anta (bindande) åtgärder och att medlemsstaterna kommer att agera om EU inte har utövat sin befogenhet eller har beslutat att inte längre agera (artikel 2.2 i EU-fördraget).

Åtgärder som ingår i ansvaret för inre marknaden kommer att omfattas av det ordinarie lagstiftningsförfarandet (artiklarna 289 och 294 i EU-fördraget), som liknar[14] det tidigare medbeslutandeförfarandet (artikel 251 i EG-fördraget).

Med Lissabonfördraget har den tidigare distinktionen mellan pelarna försvunnit. Att förebygga och bekämpa brottslighet har nu blivit en delad behörighet för EU. Detta skapar möjligheten att låta Enisa fungera som plattform för nät- och informationssäkerhetsaspekter av kampen mot cyberbrottslighet och för ett utbyte av synpunkter och bästa praxis med cyberförsvar, rättsvårdande myndigheter och myndigheter som ansvarar för skydd av personlig integritet.

3.3. Subsidiaritetsprincipen

Förslaget överensstämmer med subsidiaritetsprincipen. Nät- och informationssäkerhetspolitiken kräver en samarbetsstrategi och förslagets mål kan inte uppnås av medlemsstaterna på egen hand.

Om EU skulle välja en strategi där man inte alls ingriper i nationell nät- och informationssäkerhetspolitik skulle uppgiften överlåtas åt medlemsstaterna, trots att de befintliga informationssystemen helt klart är beroende av varandra. En åtgärd som säkrar den grad av samordning mellan medlemsstaterna som krävs för att nät- och informationssäkerhetsriskerna ska kunna hanteras på ett fungerande sätt i det gränsöverskridande sammanhang där de uppstår är därmed förenlig med subsidiaritetsprincipen. EU-åtgärder skulle dessutom öka effektiviteten i befintliga nationella åtgärder och därmed ge ett mervärde.

En samordnad nät- och informationssäkerhetspolitik präglad av samarbete kommer också att gagna skyddet av grundläggande rättigheter, i synnerhet rätten till skydd av personuppgifter och personlig integritet. Behovet av att skydda data är mycket viktigt eftersom EU-medborgarna i allt högre grad anförtror sina data till komplexa informationssystem, antingen av eget val eller av tvång, utan att de nödvändigtvis har möjlighet att göra en korrekt bedömning av de dataskyddsrisker som detta medför. När incidenter inträffar kommer de därför inte nödvändigtvis att kunna vidta lämpliga åtgärder, och det är inte heller säkert att medlemsstaterna skulle kunna klara att hantera eventuella internationella incidenter på ett effektivt sätt utan en samordning på EU-nivå.

---

13 Se ovan.

14 Det ordinarie lagstiftningsförfarandet skiljer sig framför allt när det gäller majoritetskraven i rådet och Europaparlamentet.

3.4. Proportionalitetsprincipen

Förslaget är förenligt med proportionalitetsprincipen eftersom det inte går utöver vad som är nödvändigt för att uppnå målet.

3.5. Val av regleringsform

Föreslagen regleringsform: En förordning som är direkt tillämplig i alla medlemsstater

4. BUDGETKONSEKVENSER

Förslaget kommer att påverka unionens budget.

Eftersom de uppgifter som kommer att ingå i Enisas nya mandat fastställs, förväntas det att byrån kommer att tilldelas de resurser som krävs för att den ska kunna genomföra sin verksamhet på ett tillfredsställande sätt. Utvärderingen av byrån, det omfattande samrådet med intressenter på alla nivåer och konsekvensanalysen visar en samsyn om att byråns storlek ligger under dess kritiska massa och att ökade resurser krävs. Konsekvenserna och effekterna av att öka byråns personal och budget anges i den konsekvensanalys som läggs fram tillsammans med förslaget.

EU-finansieringen efter 2013 kommer att granskas i samband med en kommissionsomfattande diskussion om alla förslag för perioden efter 2013.

5. KOMPLETTERANDE KOMMENTAR

5.1. Mandatperiod

Förordningen ska omfatta en femårsperiod.

5.2. Översynsklausul

Förordningen föreskriver att byrån ska vara föremål för en utvärdering som omfattar perioden efter den senaste utvärderingen 2007. Man kommer då att bedöma hur effektiv byrån är i förhållande till sina mål enligt förordningen, om den fortfarande är ett effektivt instrument och om mandatperioden bör förlängas ytterligare. På grundval av resultaten kommer styrelsen att utfärda rekommendationer till kommissionen om hur förordningen, byrån och dess arbetsmetoder bör ändras. För att kommissionen ska kunna utarbeta ett eventuellt förslag om utvidgning av mandatet i god tid, måste utvärderingen vara klar vid utgången av mandatperiodens andra år enligt förordningen.

5.3. Interimistiska åtgärder

Kommissionen är medveten om att Europaparlamentet och rådet kan behöva god tid för debatt om lagstiftningsförslaget och att det finns en risk för ett rättsligt vakuum om byråns nya mandat inte antas innan det nuvarande mandatet löper ut. Kommissionen föreslår därför, tillsammans med det här förslaget, en förordning om att förlänga byråns nuvarande mandat med 18 månader för att säkra tillräcklig tid för debatten och lagstiftningsprocessen.

2010/0275 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om Europeiska byrån för nät- och informationssäkerhet (Enisa)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[15],

med beaktande av Regionkommitténs yttrande[16],

efter översändande av förslaget till de nationella parlamenten,

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) Elektronisk kommunikation och infrastruktur och elektroniska tjänster har blivit mycket viktiga faktorer för ekonomisk och samhällelig utveckling. De har stor betydelse för samhället och har nu blivit grundläggande samhällsnyttigheter på samma sätt som el och vatten. Störningar kan orsaka enorma ekonomiska skador, vilket understryker betydelsen av åtgärder som ökar skyddet och motståndskraften och syftar till att säkerställa kontinuiteten för kritiska tjänster. När det gäller säkerheten för elektroniska kommunikationer, infrastrukturer och tjänster står man hela tiden inför allt större utmaningar, i synnerhet vad gäller deras integritet och tillgänglighet. Det här är ett allt större problem för samhället, inte minst för att problem kan uppstå på grund av systemens komplexitet och risken för olyckor, misstag och attacker som kan medföra konsekvenser för den fysiska infrastrukturen för tjänster av kritisk betydelse för EU-medborgarnas välfärd.

(2) Hotbilderna ändras hela tiden och säkerhetsincidenter kan skada användarnas förtroende. Allvarliga störningar av elektroniska kommunikationer, infrastrukturer och tjänster kan medföra stora ekonomiska och sociala konsekvenser, och vardagliga säkerhetsöverträdelser, problem och irritationsmoment riskerar att urholka allmänhetens förtroende för teknik, nät och tjänster.

---

15 EUT C , , s. .
16 EUT C , , s. .

(3) Det är därför viktigt för beslutsfattare, bransch och användare att det görs en regelbunden bedömning av nät- och informationssäkerhetssituationen i Europa, på grundval av tillförlitliga europeiska data.

(4) Medlemsstaternas företrädare som sammanträdde i Europeiska rådet den 13 december 2003 beslutade att Europeiska byrån för nät- och informationssäkerhet (Enisa), som skulle inrättas på grundval av kommissionens förslag, skulle ha sitt säte i en stad i Grekland som skulle fastställas av den grekiska regeringen.

(5) Europaparlamentet och rådet antog 2004 förordning (EG) nr 460/2004[17] om inrättandet av den europeiska byrån för nät- och informationssäkerhet med syftet att bidra till målet att säkerställa en hög nivå på nät- och informationssäkerhet i gemenskapen och utveckla en kultur av nät- och informationssäkerhet till förmån för medborgarna, konsumenterna, företagen och den offentliga sektorns organisationer. År 2008 antog Europaparlamentet och rådet förordning (EG) nr 1007/2008[18] som förlänger byråns mandat till mars 2012.

(6) Sedan byrån inrättades har nät- och informationssäkerhetsproblemen ändrats i takt med den teknisk utvecklingen, marknadsutvecklingen och de socioekonomiska förändringarna, och de har varit föremål för ytterligare reflektion och debatt. Som svar på de ändrade utmaningarna har EU uppdaterat sina prioriteringar för nät- och informationssäkerhetspolitiken i flera dokument, bland annat kommissionens strategi från 2006, *En strategi för ett säkert informationssamhälle – ”Dialog, partnerskap och användarinflytande”*[19], rådets resolution från 2007 om en strategi för ett säkert informationssamhälle i Europa[20] och 2009 års meddelande *om skydd av kritisk informationsinfrastruktur - ”Skydd mot storskaliga it-attacker och avbrott: förbättrad beredskap, säkerhet och motståndskraft i Europa”*[21], ordförandeskapets slutsatser från ministerkonferensen om skydd av kritisk informationsinfrastruktur samt rådets slutsatser från 2009 om en europeisk samarbetsstrategi för nät- och informationssäkerhet[22]. Man har konstaterat att byrån bör moderniseras och stärkas för att framgångsrikt kunna bidra till de europeiska institutionernas och medlemsstaternas insatser för att utveckla en europeisk kapacitet för att hantera nät- och informationssäkerhetsproblem. Mer nyligen antog kommissionen en digital agenda för Europa[23], som centralt initiativ inom strategin Europa 2020. Denna övergripande agenda syftar till att utnyttja och utveckla informations- och kommunikationsteknikens potential så att den kan omvandlas till hållbar tillväxt och innovation. Ett viktigt mål för den digitala agendan är att bygga upp förtroendet för och tilltron till informationssamhället, och den omfattar en mängd åtgärder som kommissionen ska vidta inom detta område, inklusive detta förslag.

(7) För inre marknadsåtgärder inom området säkerhet för elektronisk kommunikation och, mer allmänt, nät- och informationssäkerhet krävs olika former av tekniska och

---

17 EUT L 77, 13.3.2004, s. 1.
18 EUT L 293, 31.10.2008, s. 1.
19 KOM(2006) 251, 31.5.2006.
20 Rådets resolution av den 22 mars 2007 om en strategi för ett säkert informationssamhälle i Europa, EUT C 68, 24.3.2007, s. 1
21 KOM(2009) 149, 30.3.2009.
22 Rådets resolution av 18 december 2009 om en strategi för ett säkert informationssamhälle i Europa, EUT C 321, 29.12.2009, s. 1.
23 KOM(2010) 245, 19.5.2010.

organisatoriska tillämpningar hos medlemsstaterna och kommissionen. Det faktum att dessa krav tillämpas på många olika sätt kan leda till ineffektivitet och skapa hinder på den inre marknaden. Därför behövs ett expertcentrum på EU-nivå som tillhandahåller riktlinjer, rådgivning och vid behov bistånd i nät- och informationssäkerhetsfrågor, vilket medlemsstaterna och EU-institutionerna kan utnyttja. Byrån kan tillgodose dessa behov genom att utveckla och upprätthålla en hög nivå av expertis och bistå medlemsstaterna, kommissionen och därmed även näringslivet, för att hjälpa dem att uppfylla nät- och informationssäkerhetskraven i lagar och andra förordningar, och därigenom bidra till en välfungerande inre marknad.

(8) Byrån bör utföra de uppgifter som den tilldelats genom den nuvarande EU-lagstiftningen inom området elektronisk kommunikation och, rent allmänt, bidra till ökad säkerhet för elektronisk kommunikation och bland annat tillhandahålla expertis och rådgivning och främja utbyte av god praxis.

(9) Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv)[24] föreskriver att företag som tillhandahåller allmänt tillgängliga elektroniska kommunikationsnät eller kommunikationstjänster vidtar lämpliga åtgärder för att säkerställa deras integritet och säkerhet; direktivet inför också anmälningskrav avseende säkerhetsöverträdelser och integritetsförlust. När så är lämpligt ska byrån även underrättas av de nationella regleringsmyndigheterna som också ska lämna en årlig rapport till kommissionen som sammanfattar de anmälningar som inkommit och åtgärder som vidtagits. Enligt direktiv 2002/21/EG ska byrån dessutom bidra till harmoniseringen av lämpliga tekniska och organisatoriska säkerhetsåtgärder genom att utfärda yttranden.

(10) Enligt Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation)[25] ska en leverantör av en allmänt tillgänglig elektronisk kommunikationstjänst vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa säkerheten i sina tjänster samt konfidentialitet vid kommunikation och för därmed förbundna trafikuppgifter. Genom direktiv 2002/58/EG införs informations- och anmälningskrav avseende personuppgiftsbrott för leverantörer av elektroniska kommunikationstjänster. Där åläggs också kommissionen att konsultera byrån i samband med antagandet av tekniska genomförandeåtgärder beträffande de omständigheter, former och förfaranden som kan tillämpas på informations- och anmälningskrav. Enligt Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter[26] ska medlemsstaterna föreskriva att den registeransvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från förstöring genom olyckshändelse eller otillåtna handlingar eller förlust genom olyckshändelse samt mot ändringar, otillåten spridning av eller otillåten tillgång till uppgifterna, särskilt om behandlingen innefattar överföring av uppgifter i ett nät, och mot varje annat slag av otillåten behandling.

---

[24] EGT L 108, 24.4.2002, s. 33.
[25] EGT L 201, 31.7.2002, s. 37.
[26] EGT L 281, 23.11.1995, s. 31.

(11) Byrån bör bidra till en hög nivå på nät- och informationssäkerheten i gemenskapen och till att utveckla en kultur för nät- och informationssäkerhet till gagn för medborgarna, konsumenterna, företagen och den offentliga sektorns organisationer i Europeiska unionen, och på så sätt bidra till att den inre marknaden fungerar väl.

(12) Byråns uppgifter bör visa hur den ska uppnå sina mål och samtidigt möjliggöra flexibilitet i verksamheten. Byråns uppgifter bör omfatta insamling av information och data som behövs för analys av risker förknippade med säkerheten och motståndskraften för elektroniska kommunikationsinfrastrukturer och kommunikationstjänster och för att i samarbete med medlemsstaterna göra en bedömning av nät- och informationssäkerhetssituationen i Europa. Byrån bör säkra samordning med medlemsstaterna och förbättra samarbetet mellan aktörer i Europa, i synnerhet genom att engagera behöriga nationella organ och experter från den privata sektorn inom området nät- och informationssäkerhet i verksamheten. Byrån bör bistå kommissionen och medlemsstaterna i deras dialog med branschen för att lösa säkerhetsrelaterade problem i hårdvaru- och mjukvaruprodukter och därigenom bidra till en samarbetsstrategi för nät- och informationssäkerhet.

(13) Byrån bör fungera som en referenspunkt och skapa förtroende genom sin opartiskhet samt genom kvaliteten på de råd och den information den tillhandahåller, öppenheten i dess förfaranden och arbetssätt samt dess skickliga sätt att utföra sina uppgifter. Byrån bör bygga vidare på de ansträngningar som gjorts nationellt och på EU-nivå och därför utföra sina uppgifter i fullständigt samarbete med medlemsstaterna samt vara öppen för kontakter med näringslivet och andra berörda intressenter. Byrån bör också bygga vidare på synpunkter från och samarbete med den privata sektorn, som spelar en viktig roll för säkra elektroniska kommunikationsinfrastrukturer och kommunikationstjänster.

(14) Kommissionen har tagit initiativ till ett europeiskt offentligprivat EU-partnerskap för motståndskraft som flexibel europeiska ram för IKT-infrastrukturens motståndskraft, där byrån bör fungera som främjare och föra samman intressenter från offentlig och privat sektor för att diskutera den offentliga politikens prioriteringar, ekonomiska och marknadsanknutna dimensioner av utmaningar och åtgärder för IKT-infrastrukturens motståndskraft och för att fastställa intressenternas ansvar.

(15) Byrån bör ge kommissionen råd i form av yttranden och tekniska och socioekonomiska analyser, på begäran av kommissionen eller på eget initiativ, för att bidra till politikens utveckling inom området nät- och informationssäkerhet. Byrån bör också på begäran bistå medlemsstaterna och EU:s institutioner och organ i deras arbete för att utveckla nät- och informationssäkerhetspolitiken och -kapaciteten.

(16) Byrån bör bistå medlemsstaterna och EU-institutionerna i deras arbete för att bygga upp och förbättra den gränsöverskridande kapaciteten och beredskapen för att förebygga, spåra, mildra och reagera på nät- och informationssäkerhetsproblem och –incidenter, i detta hänseende bör byrån främja samarbete mellan medlemsstaterna och mellan medlemsstaterna och kommissionen. Därför bör byrån inta en aktiv hållning och stödja medlemsstaterna i deras kontinuerliga insatser för att förbättra sin insatskapacitet och för att organisera och leda nationella och europeiska övningar för säkerhetsincidenter.

(17) Direktiv 95/46/EG avgör behandlingen av personuppgifter enligt denna förordning.

(18) För att bättre förstå utmaningarna inom området nät- och informationssäkerhet behöver byrån analysera befintliga och kommande risker. Därför bör byrå i samarbete med medlemsstaterna och, om lämpligt, statistikorgan samla in relevant information. Byrån bör också bistå medlemsstaterna och EU:s institutioner och organ i deras arbete med att samla in, analysera och sprida nät- och informationssäkerhetsdata.

(19) När byrån utför sina övervakningsuppgifter i EU bör den främja ett samarbete mellan EU och medlemsstater för att bedöma nät- och informationssäkerhetssituationen i Europa och bidra till bedömningsarbetet i samarbete med medlemsstaterna.

(20) Byrån bör främja ett samarbete mellan medlemsstaternas behöriga offentliga organ, i synnerhet för att stödja utveckling och utbyte av god praxis samt standarder för utbildningsprogram och informationskampanjer. Ett ökat informationsutbyte mellan medlemsstaterna kommer att underlätta sådana åtgärder. Byrån bör också stödja samarbete mellan offentliga och privata aktörer på EU-nivå, bland annat genom att främja informationsutbyte, kampanjer för att öka medvetenheten och utbildningsprogram.

(21) Effektiva säkerhetsriktlinjer bör bygga på välutvecklade metoder för riskbedömning, både inom den offentliga och den privata sektorn. Metoder och förfaranden för riskbedömning används på olika nivåer men det saknas gemensamma metoder för effektiv tillämpning. Främjandet och utvecklingen av bästa praxis för riskbedömning och för interoperabla lösningar för riskhantering inom organisationer i den offentliga och privata sektorn kommer att höja säkerhetsnivån för nät- och informationssystemen i Europa. Därför bör byrån stödja samarbete mellan offentliga och privata aktörer på EU-nivå och främja deras insatser för utveckling och tillämpning av riskhanteringsstandarder och mätbar säkerhet för elektroniska produkter, system, nät och tjänster.

(22) Byrån bör i sitt arbete dra nytta av pågående forskning, utveckling och teknisk bedömning, i synnerhet sådan verksamhet som bedrivs inom Europeiska unionens olika forskningsinitiativ.

(23) I de fall då det är lämpligt och gagnar fullgörandet av byråns verksamhetsområde, mål och uppgifter bör byrån dela erfarenheter och allmän information med sådana organ och byråer som inrättats genom gemenskapslagstiftningen och som arbetar med nät- och informationssäkerhet.

(24) I samarbetet med rättsvårdande organ om cyberbrottslighetens säkerhetsaspekter bör byrån använda existerande informationskanaler och etablerade nät som de kontaktpunkter som nämns i föreslaget till Europaparlamentets och rådets direktiv om angrepp mot informationssystem, som upphäver rambeslut 2005/222/RIF, eller Europol Heads of High Tech Crime Units Task Force.

(25) För att säkerställa att alla byråns mål uppnås bör den upprätthålla kontakter med brottsbekämpande organ och myndigheter som ansvarar för skydd av personlig integritet, för att belysa och på ett korrekt sätt hantera nät- och informationssäkerhetsaspekterna av kampen mot cyberbrottslighet. Företrädare för dessa myndigheter bör tas med som fullvärdiga intressenter i byrån och företrädas i byråns ständiga intressentgrupp.

(26) Nät- och informationssäkerhetsproblemen är globala. Det behövs ett tätare internationellt samarbete för att förbättra säkerhetsstandarder, öka informationsutbytet och främja en gemensam global syn på nät- och informationssäkerhetsfrågor. Därför bör byrån stödja samarbete med tredjeländer och internationella organisationer, när så är lämpligt i samarbete med Europeiska avdelningen för yttre åtgärder (EEAS).

(27) Byrån bör i utförandet av sina arbetsuppgifter varken inkräkta på eller förekomma, hindra eller dubblera de relevanta befogenheter och arbetsuppgifter som tillkommer de nationella regleringsmyndigheterna enligt direktiven om elektroniska kommunikationsnät och kommunikationstjänster, Europeiska gruppen av regleringsmyndigheter för nät och tjänster inom området elektronisk kommunikation som inrättades genom Europaparlamentets och rådets förordning 1211/2009[27], kommunikationskommittén enligt direktiv 2002/21/EG, de europeiska standardiseringsorganen, de nationella standardiseringsorganen, den permanenta kommittén enligt Europaparlamentets och rådets direktiv 98/34/EG av den 22 juni 1998 om ett informationsförfarande beträffande tekniska standarder och föreskrifter och beträffande föreskrifter för informationssamhällets tjänster[28] samt medlemsstaternas tillsynsmyndigheter för skyddet av enskilda personer när det gäller behandling av personuppgifter samt den fria rörligheten för sådana uppgifter.

(28) För att säkerställa att byrån är effektiv bör medlemsstaterna och kommissionen vara företrädda i styrelsen, som bör fastställa den allmänna inriktningen på byråns verksamhet och se till att den utför sina uppgifter i enlighet med denna förordning. Styrelsen ha de nödvändiga befogenheterna för att fastställa budgeten och kontrollera att den genomförs, anta lämpliga finansiella bestämmelser, utarbeta klara och tydliga förfaranden för byråns beslutsfattande, anta byråns arbetsprogram, anta sin egen arbetsordning och byråns interna verksamhetsregler samt besluta om förlängning eller avslutande av den verkställande direktörens mandatperiod. Styrelsen bör kunna inrätta arbetsgrupper som kan bistå den i dess uppgifter; sådana arbetsgrupper skulle t.ex. kunna utarbeta byråns beslut eller övervaka genomförandet av besluten.

(29) För att byrån ska fungera väl bör den verkställande direktören utses på grundval av meriter, dokumenterad skicklighet i förvaltning och ledarskap samt kompetens och erfarenheter som rör nät- och informationssäkerhet; dessutom bör han/hon vara helt oberoende vid organisationen av byråns interna arbete. Den verkställande direktören bör därför utarbeta ett förslag till arbetsprogram för byrån, efter samråd med kommissionens avdelningar, och vidta alla åtgärder som är nödvändiga för att säkerställa att byråns arbetsprogram genomförs på rätt sätt. Han/hon bör varje år utarbeta ett utkast till årsrapport som föreläggs styrelsen och göra ett förslag till beräkning av byråns inkomster och utgifter samt genomföra budgeten.

(30) Den verkställande direktören bör ha möjlighet att inrätta tillfälliga arbetsgrupper som i synnerhet ska behandla vetenskapliga, tekniska, rättsliga eller socioekonomiska frågor. Vid inrättandet av sådana arbetsgrupper bör den verkställande direktören inhämta synpunkter från och utnyttja sådan relevant extern expertis som krävs för att byrån ska få tillgång till den mest aktuella informationen om säkerhetsproblem i det föränderliga informationssamhället. Byrån bör se till att de tillfälliga arbetsgruppernas medlemmar väljs utifrån högsta krav på expertkunskaper, med beaktande av att det, utifrån de

---

[27] EUT L 337, 18.12.2009, s.1.
[28] EGT L 204, 21.7.1998, s. 37.

specifika frågor som berörs, ska finnas en representativ balans mellan medlemsstaternas förvaltningar, privata sektorn (inklusive branschen), användare och akademiska experter på nät- och informationssäkerhet. Byrån får vid behov bjuda in enskilda experter som har erkänd kompetens från det relevanta området för att delta i arbetsgruppens verksamhet, från fall till fall. Deras utgifter bör bekostas av byrån i enlighet med dess interna regler och gällande budgetförordningar.

(31) Byrån bör ha en ständig intressentgrupp som rådgivande organ, för att säkerställa en regelbunden dialog med den privata sektorn, konsumentorganisationer och andra berörda aktörer. Den ständiga intressentgruppen, som inrättas och leds av styrelsen, bör koncentrera sig på frågor som är relevanta för alla berörda intressenter och uppmärksamma byrån på dem. Den verkställande direktören kan, vid behov och i enlighet med mötenas föredragningslista, bjuda in företrädare för Europaparlamentet och andra berörda organ att delta i gruppens möten.

(32) Byrån ska verka i enlighet med i) subsidiaritetsprincipen och därvid säkra en lämplig grad av samordning mellan medlemsstaterna när det gäller nät- och informationssäkerhetsfrågor och göra nationell politik effektivare, och därmed tillföra ett mervärde, och ii) proportionalitetsprincipen, och inte gå utöver vad som är nödvändigt för att uppnå de mål som fastställs i den här förordningen.

(33) Byrån bör tillämpa relevant EU-lagstiftning om allmänhetens tillgång till handlingar enligt Europaparlamentets och rådets förordning (EG) nr 1049/2001[29] och skyddet av enskilda när det gäller behandling av personuppgifter enligt Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter[30].

(34) Inom ramen för sitt verksamhetsområde, sina mål och utförandet av sina uppgifter bör byrån i synnerhet iaktta de bestämmelser som gäller för EU:s institutioner och den nationella lagstiftningen om hanteringen av känsliga dokument. Styrelsen bör ha befogenhet att fatta ett beslut som tillåter byrån att hantera sekretessbelagda uppgifter.

(35) För att garantera byråns fulla oberoende och självständighet anses det nödvändigt att den har en egen budget där intäkterna främst består av ett bidrag från EU och bidrag från tredjeländer som deltar i byråns arbete. Värdmedlemsstaten, eller varje annan medlemsstat, bör ha rätt att lämna frivilliga bidrag till byråns intäkter. EU:s budgetförfarande bör även i fortsättningen tillämpas på de bidrag som belastar Europeiska unionens allmänna budget. Dessutom bör revisionsrätten granska räkenskaperna.

(36) Byrån bör efterträda Enisa som inrättades genom förordning nr 460/2004. I enlighet med ramarna i det beslut som fattades av medlemsstaternas företrädare när de sammanträdde i Europeiska rådet den 13 december 2003 bör värdmedlemsstaten bibehålla och utveckla de nuvarande praktiska arrangemangen för att säkra en smidig

---

[29] Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar, EGT L 145, 31.5.2001, s. 43.

[30] Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, EGT L 8, 12.1.2001, s. 1.

och effektiv drift av byrån, i synnerhet med beaktande av byråns samarbete med och bistånd till kommissionen, medlemsstaterna och deras behöriga organ, övriga EU-institutioner och EU-organ och offentliga och privata intressenter i hela Europa.

(37) Byrå bör inrättas för en begränsad period. Man bör utvärdera byråns verksamhet utifrån dess effektivitet i förhållande till målen och dess arbetsmetoder, för att fastställa om byråns mål fortfarande är giltiga och, på grundval av detta, om dess verksamhet bör förlängas ytterligare.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

AVSNITT 1 VERKSAMHETSOMRÅDE, MÅL OCH UPPGIFTER

Artikel 1
Syfte och tillämpningsområde

1. Genom denna förordning inrättas Europeiska byrån för nät- och informationssäkerhet (nedan kallad *byrån)*, som ska bidra till en hög nivå på nät- och informationssäkerhet i EU, öka medvetenheten om dessa frågor och utveckla en kultur av nät- och informationssäkerhet i samhället till förmån för medborgarna, konsumenterna, företagen och den offentliga sektorns organisationer i Europeiska unionen och på det sättet bidra till att den inre marknaden fungerar väl.

2. Byråns mål och uppgifter ska inte påverka medlemsstaternas befogenheter i fråga om nät- och informationssäkerhet, särskilt inte verksamhet som berör allmän säkerhet, försvar, statssäkerhet (också statens ekonomiska välstånd, när frågorna har anknytning till statens säkerhet) och staternas verksamhet på strafflagstiftningens område.

3. I denna förordning avser *nät- och informationssäkerhet* förmågan hos ett nät eller ett informationssystem att, vid en viss tillförlitlighetsnivå, tåla olyckshändelser, olagliga handlingar eller illvilligt uppträdande som äventyrar tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda data och besläktade tjänster som tillhandahålls av eller är tillgängliga via dessa nät och system.

Artikel 2
Mål

1. Byrån ska bistå kommissionen och medlemsstaterna för att uppfylla kraven i lagar och andra förordningar avseende nät- och informationssäkerhet i nuvarande eller framtida EU-lagstiftning och på så sätt bidra till att den inre marknaden fungerar väl.

2. Byrån ska förbättra EU:s och medlemsstaternas kapacitet och beredskap för att förebygga, spåra och reagera på nät- och informationssäkerhetsproblem.

3. Byrån ska utveckla och upprätthålla en hög nivå av expertis och använda denna expertis för att främja ett brett samarbete mellan aktörer från offentlig och privat sektor.

Artikel 3
Uppgifter

1. För det syfte som fastställs i artikel 1 ska byrån utföra följande uppgifter:

(a) Bistå kommissionen, på dess begäran eller på eget initiativ, i frågor som rör utvecklingen av nät- och informationssäkerhetspolitiken, genom att tillhandahålla råd och yttranden och tekniska och socioekonomiska analyser, och med förberedande arbeten inför utveckling och uppdatering av EU-lagstiftning inom området nät- och informationssäkerhet.

(b) Främja samarbete mellan medlemsstaterna och mellan medlemsstaterna och kommissionen i deras insatser med en gränsöverskridande dimension för att förebygga, spåra och hantera nät- och informationssäkerhetsincidenter.

(c) Bistå medlemsstaterna och EU:s institutioner och organ i deras arbete med att samla in, analysera och sprida nät- och informationssäkerhetsdata.

(d) I samarbete med medlemsstaterna och EU-institutionerna bedöma nät- och informationssäkerhetssituationen i Europa.

(e) Stödja samarbete mellan behöriga offentliga organ i Europa, och framför allt stödja deras insatser för att utveckla och utbyta god praxis och standarder.

(f) Bistå EU och medlemsstaterna för att främja användning av god praxis i fråga om riskhantering och säkerhet samt standarder för elektroniska produkter, system och tjänster.

(g) Stödja samarbete mellan offentliga och privata aktörer på EU-nivå, bland annat genom att främja informationsutbyte och åtgärder för att öka medvetenheten, och underlätta deras insatser för att utveckla och använda standarder för riskhantering och för säkerheten för elektroniska produkter, nät och tjänster.

(h) Främja dialog och utbyte av god praxis mellan offentliga och privata intressenter inom området nät- och informationssäkerhet, även när det gäller olika aspekter av bekämpandet av cyberbrottslighet, och bistå kommissionen i utvecklingen av strategier som beaktar nät- och informationssäkerhetsaspekter av bekämpandet av cyberbrottslighet.

(i) På begäran bistå medlemsstaterna och EU:s institutioner och organ i deras arbete för att utveckla kapaciteten för spårning, analys och insatser inom området nät- och informationssäkerhet.

(j) Stödja EU:s dialog och samarbete med tredjeländer och internationella organisationer, när så är lämpligt i samarbete med Europeiska utrikestjänsten, för att främja internationellt samarbete och en gemensam global syn på hur nät- och informationssäkerhetsfrågor ska hanteras.

(k) Utföra de uppgifter som byrån tilldelas genom EU-lagstiftning.

AVSNITT 2 ORGANISATION

Artikel 4
Byråns organ

Byrån ska bestå av

(a) en styrelse,

(b) en verkställande direktör med erforderlig personal, och

(c) en ständig intressentgrupp.

Artikel 5
Styrelse

1. Styrelsen ska fastställa de allmänna riktlinjerna för byråns arbete och se till att byrån agerar i enlighet med de regler och principer som fastställs i denna förordning. Styrelsen ska även se till att byråns arbete överensstämmer med det arbete som utförs av medlemsstaterna och på EU-nivå.

2. Styrelsen ska anta sin arbetsordning efter överenskommelse med berörda kommissionsavdelningar.

3. Styrelsen ska anta byråns interna verksamhetsregler efter överenskommelse med berörda kommissionsavdelningar. Reglerna ska offentliggöras.

4. Styrelsen ska utse den verkställande direktören i enlighet med artikel 10.2 och får entlediga den verkställande direktören. Styrelsen ska utöva disciplinär makt över direktören.

5. Styrelsen ska anta byråns arbetsprogram i enlighet med artikel 13.3 och årsrapporten om byråns verksamhet under föregående år i enlighet med artikel 14.2.

6. Styrelsen ska anta de finansiella bestämmelser som är tillämpliga på byrån. Bestämmelserna får inte avvika från kommissionens förordning (EG, Euratom) nr 2343/2002 av den 19 november 2002 med rambudgetförordning för de gemenskapsorgan som avses i artikel 185 i rådets förordning (EG, Euratom) nr 1605/2002 med budgetförordning för Europeiska gemenskapernas allmänna budget[31] om inte byråns särskilda förvaltningsbehov kräver detta och kommissionen har godkänt detta i förväg.

7. Styrelsen ska, i samförstånd med kommissionen och i enlighet med artikel 110 i tjänsteföreskrifterna, anta lämpliga tillämpningsföreskrifter.

8. Styrelsen får inrätta arbetsorgan bestående av styrelseledamöter som ska biträda den vid utförandet av dess uppdrag och i arbetet med att förbereda och övervaka genomförandet av styrelsens beslut.

---

[31] EGT L 357, 31.12.2002, s. 72.

9. Styrelsen får anta den fleråriga personalplanen efter samråd med kommissionens avdelningar och efter att ha informerat budgetmyndigheten.

Artikel 6
Styrelsens sammansättning

1. Styrelsen ska bestå av en företrädare för varje medlemsstat, tre ledamöter som utses av kommissionen samt tre företrädare utan rösträtt som ska utnämnas av rådet på förslag av kommissionen, vilka var och en ska representera en av nedanstående grupper:

(a) IKT-branschen.

(b) Konsumentgrupper.

(c) Sakkunniga på nät- och informationssäkerhet från akademiska världen.

2. Styrelseledamöterna och deras suppleanter ska utses på grundval av relevant erfarenhet och sakkunskap inom området för nät- och informationssäkerhet.

3. Mandatperioden för företrädarna för de grupper som avses i 1 a, 1 b och 1 c ska vara fyra år. Mandatperioden kan förnyas en gång. Om en företrädare lämnar sin anknytning med respektive intressegrupp ska kommissionen utse en ersättare.

Artikel 7
Styrelsens ordförande

Styrelsen ska bland sina ledamöter utse en ordförande och en vice ordförande för en period på tre år som får förnyas. Vice ordföranden ska inträda i ordförandens ställe om den senare inte kan fullgöra sina plikter.

Artikel 8
Sammanträden

1. Styrelsens sammanträden ska sammankallas av dess ordförande.

2. Styrelsen ska hålla två ordinarie sammanträden per år. Den ska också hålla extra sammanträden på begäran av ordföranden eller då minst en tredjedel av de röstberättigade ledamöterna så begär.

3. Verkställande direktören ska delta i styrelsemötena utan rösträtt.

Artikel 9
Omröstning

1. Styrelsen ska fatta beslut genom en majoritet av sina röstberättigade ledamöter.

2. Två tredjedelars majoritet av de röstberättigade styrelseledamöterna krävs vid antagandet av dess arbetsordning, byråns interna verksamhetsregler, budgeten, det årliga

arbetsprogrammet samt när verkställande direktör utnämns, får sin mandatperiod förlängd eller avsätts.

Artikel 10
Den verkställande direktören

1. Byrån ska ledas av en verkställande direktör som ska ha en oberoende ställning i utförandet av sina arbetsuppgifter.

2. Den verkställande direktören ska utses och entledigas av styrelsen. Utnämningen ska göras från en lista med kandidater som föreslås av kommissionen för en femårsperiod, på grundval av meriter, dokumenterad skicklighet i förvaltning och ledarskap samt kompetenser och erfarenheter. Den kandidat som styrelsen väljer kan före utnämningen ombes att göra ett uttalande inför behörigt utskott i Europaparlamentet och besvara frågor från utskottsledamöterna.

3. Under de nio månaderna före periodens utgång ska kommissionen göra en utvärdering. I utvärderingen ska kommissionen särskilt bedöma

– den verkställande direktörens arbete, och

– byråns uppgifter och behov under de närmaste åren.

4. Styrelsen får på förslag av kommissionen, med beaktande av utvärderingsrapporten och endast i de fall det kan motiveras på grund av byråns uppgifter och behov, förlänga direktörens mandatperiod med högst tre år.

5. Styrelsen ska underrätta Europaparlamentet om sin avsikt att förlänga den verkställande direktörens mandatperiod. Under den månad som föregår förlängningen av mandatperioden kan den verkställande direktören ombes att göra ett uttalande inför Europaparlamentets behöriga utskott och besvara frågor från utskottsledamöterna.

6. Om mandatperioden inte förlängs ska den verkställande direktören sitta kvar till dess att en efterträdare har utsetts.

7. Den verkställande direktören ska ha ansvaret för

(a) myndighetens dagliga förvaltning,

(b) genomförandet av arbetsprogrammet och styrelsens beslut,

(c) säkerställandet av att byrån genomför sin verksamhet i enlighet med användarnas krav, särskilt med avseende på om de tjänster som tillhandahålls fyller deras behov,

(d) alla specifika personalfrågor och säkerställandet av att de är förenliga med styrelsens allmänna riktlinjer och med styrelsens beslut av allmän art,

(e) utvecklingen och upprätthållandet av kontakter med EU:s institutioner och organ,

(f) utvecklingen och upprätthållandet av kontakter med näringslivet och konsumentorganisationer för att garantera en regelbunden dialog med berörda intressenter, och

(g) andra uppgifter som han eller hon tilldelas genom denna förordning.

8. När så är nödvändigt och inom ramen för byråns mål och uppgifter får den verkställande direktören inrätta arbetsgrupper bestående av experter. Styrelsen ska underrättas i förväg. Förfarandena för att fastställa sammansättningen av dessa grupper, hur experter ska utses av den verkställande direktören och hur de tillfälliga arbetsgrupperna ska arbeta ska anges i byråns interna verksamhetsregler.

9. Den verkställande direktören ska se till att styrelsen vid behov får tillgång till administrativ stödpersonal och andra resurser.

Artikel 11
Ständig intressentgrupp

1. Styrelsen ska på förslag av den verkställande direktören inrätta en ständig intressentgrupp bestående av experter som företräder berörda intressenter, exempelvis informations- och kommunikationstekniksbranschen, konsumentgrupper, experter på nät- och informationssäkerhet från den akademiska världen och rättsvårdande myndigheter samt myndigheter med ansvar för skydd av personlig integritet.

2. Förfarandena för att fastställa antalet medlemmar i gruppen, dess sammansättning, hur medlemmar utses av den verkställande direktören och hur gruppen ska arbeta ska anges i byråns interna verksamhetsregler och offentliggöras.

3. Den verkställande direktören ska vara gruppens ordförande.

4. Mandatperioden för gruppens medlemmar ska vara två och ett halvt år. Styrelseledamöter får inte vara medlemmar i gruppen. Kommissionens personal får närvara vid gruppens möten och delta i dess arbete.

5. Gruppen ska ge byrån råd om genomförandet av dess verksamhet. Gruppen ska i synnerhet ge den verkställande direktören råd om utarbetandet av förslaget till byråns arbetsprogram och om kommunikationen med berörda intressenter om alla frågor kopplade till arbetsprogrammet.

AVSNITT 3 VERKSAMHET

Artikel 12
Arbetsprogram

1. Byrån ska genomföra sin verksamhet i enlighet med sitt arbetsprogram, som ska innehålla all planerad verksamhet. Arbetsprogrammet ska inte hindra byrån från att ta på sig oförutsedda uppgifter som omfattas av byråns mål och uppgifter och ryms inom budgetramarna. Den verkställande direktören ska informera styrelsen om sådana verksamheter som inte ingår i arbetsprogrammet.

2. Den verkställande direktören ska ha ansvaret för att utarbeta utkastet till byråns arbetsprogram efter samråd med kommissionens avdelningar. Före den 15 mars varje år ska den verkställande direktören lämna ett förslag till arbetsprogram för följande år till styrelsen.

3. Före den 30 november varje år ska styrelsen anta byråns arbetsprogram för det kommande året i samråd med kommissionens avdelningar. Arbetsprogrammet ska innehålla en flerårig planering. Styrelsen ska se till att arbetsprogrammet överensstämmer med byråns mål och med gemenskapens prioriteringar för lagstiftning och politiska åtgärder inom området nät- och informationssäkerhet.

4. Arbetsprogrammet ska organiseras i enlighet med principen om verksamhetsbaserad förvaltning (*Activity-Based Management, ABM*). Arbetsprogrammet ska vara i linje med beräkningen av byråns intäkter och utgifter och byråns budget för samma budgetår.

5. När styrelsen antagit arbetsprogrammet ska den verkställande direktören vidarebefordra det till Europaparlamentet, rådet, kommissionen och medlemsstaterna, samt låta offentliggöra det.

Artikel 13
Allmän rapport

1. Den verkställande direktören ska varje år förelägga styrelsen ett utkast till årsrapport som omfattar alla byråns verksamheter under föregående år.

2. Före den 31 mars varje år ska styrelsen anta årsrapporten om byråns verksamhet under föregående år.

3. Efter det att styrelsen har antagit byråns årsrapport ska den verkställande direktören vidarebefordra den till Europaparlamentet, rådet, kommissionen, revisionsrätten, Europeiska ekonomiska och sociala kommittén och Regionkommittén, samt låta offentliggöra denna.

Artikel 14
Framställningar till byrån

1. Förfrågningar om råd och stöd som omfattas av byråns mål och arbetsuppgifter ska ställas till den verkställande direktören tillsammans med bakgrundsinformation som förklarar ärendet i fråga. Den verkställande direktören ska informera styrelsen om de förfrågningar som inkommit och sedan om den uppföljning som gjorts. Om byrån avvisar en begäran ska detta motiveras.

2. De förfrågningar som avses i punkt 1 får göras av

(a) Europaparlamentet,

(b) rådet,

(c) kommissionen, och

(d) behöriga organ utsedda av medlemsstaterna, t.ex. en nationell regleringsmyndighet enligt definitionen i artikel 2 i direktiv 2002/21/EG.

3. De praktiska arrangemangen för tillämpning av punkterna 1 och 2, särskilt vad gäller framställning, prioritering och uppföljning av förfrågningar ställda till byrån samt information till styrelsen om dessa, ska fastställas av styrelsen och anges i byråns interna verksamhetsregler.

Artikel 15
Redovisning av intressen

1. Den verkställande direktören och tjänstemän som är tillfälligt utlånade från medlemsstaterna ska göra en skriftlig åtagandeförklaring och en skriftlig förklaring som visar att det inte föreligger några direkta eller indirekta intressekonflikter som skulle kunna inverka negativt på deras oberoende.

2. Externa sakkunniga som deltar i tillfälliga arbetsgrupper ska vid varje möte redovisa eventuella intressen som kan påverka deras oberoende i förhållande till frågorna på dagordningen och avhålla sig från att delta i diskussioner om sådana frågor.

Artikel 16
Insyn

1. Byrån ska se till att dess arbete utförs med en hög grad av öppenhet och i enlighet med artiklarna 13 och 14.

2. Byrån ska se till att allmänheten och eventuella berörda parter får objektiv, tillförlitlig och lättillgänglig information, framför allt, när så är lämpligt, om resultaten av dess arbete. Den ska också offentliggöra intresseförklaringarna från verkställande direktören och tjänstemän som är tillfälligt utlånade från medlemsstaterna samt de intresseförklaringar som avges av sakkunniga i förhållande till frågor på dagordningarna till de tillfälliga arbetsgruppernas möten.

3. Styrelsen får, på förslag från den verkställande direktören, ge andra berörda parter tillstånd att observera delar av byråns verksamhet.

4. Byrån ska i sina interna verksamhetsregler fastställa hur de regler om öppenhet som avses i punkterna 1 och 2 ska tillämpas praktiskt.

Artikel 17
Sekretess

1. Byrån ska inte för tredje part röja uppgifter som den behandlar eller mottar för vilka en konfidentiell behandling har begärts, utan att detta påverkar tillämpningen av artikel 14.

2. Ledamöterna i styrelsen, den verkställande direktören, den ständiga intressentgruppen, de externa sakkunniga som deltar i olika tillfälliga arbetsgrupper och byråns personal, inbegripet tjänstemän som är tillfälligt utlånade från medlemsstaterna, ska omfattas av tystnadsplikt enligt artikel 339 i fördraget, även efter det att deras uppdrag upphört.

3. Byrån ska i sina interna verksamhetsregler fastställa hur de regler om tystnadsplikt som avses i punkterna 1 och 2 ska tillämpas praktiskt.

4. Styrelsen får besluta om att tillåta byrån att hantera sekretessbelagda uppgifter. I sådana fall ska styrelsen efter överenskommelse med berörda kommissionsavdelningar anta interna verksamhetsregler som tillämpar säkerhetsprinciperna i kommissionens beslut 2001/844/EG,

EKSG,Euratom av den 29 november 2001 om ändring av de interna stadgarna[32]. Detta ska bland annat omfatta bestämmelser om utbyte, behandling och lagring av sekretessbelagda uppgifter.

Artikel 18
Tillgång till handlingar

1. Förordning (EG) nr 1049/2001 ska tillämpas på de handlingar som finns hos byrån.

2. Styrelsen ska vidta åtgärder för att tillämpa förordning (EG) nr 1049/2001 inom sex månader från det att byrån inrättats.

3. Beslut som fattas av byrån i enlighet med artikel 8 i förordning (EG) nr 1049/2001 får prövas genom ett klagomål till ombudsmannen eller genom att talan väcks vid Europeiska unionens domstol i enlighet med artikel 228 respektive artikel 263 i fördraget.

AVSNITT 4 FINANSIELLA BESTÄMMELSER

Artikel 19
Antagande av budgeten

1. Byråns inkomster ska bestå av ett bidrag från Europeiska unionen, bidrag från tredje länder som deltar i byråns arbete i enlighet med artikel 29 och bidrag från medlemsstaterna.

2. Byråns utgifter ska täcka kostnaderna för personal, administrativt och tekniskt stöd, infrastruktur och drift samt utgifter i samband med avtal som ingås med tredje part.

3. Senast den 1 mars varje år ska den verkställande direktören göra ett förslag till beräkning av byråns inkomster och utgifter för det därpå följande budgetåret, och ska översända det till styrelsen tillsammans med ett förslag till tjänsteförteckning.

4. Inkomster och utgifter ska vara i balans.

5. Varje år ska styrelsen på grundval av det förslag till beräkning av inkomster och utgifter som utarbetats av den verkställande direktören lägga fram en beräkning av byråns inkomster och utgifter för det därpå följande budgetåret.

6. Denna beräkning av inkomster och utgifter, som även ska omfatta ett utkast till tjänsteförteckning och ett utkast till arbetsprogram, ska styrelsen senast den 31 mars överlämna till kommissionen och de stater med vilka gemenskapen slutit avtal i enlighet med artikel 24.

7. Kommissionen ska vidarebefordra beräkningen av inkomster och utgifter till Europaparlamentet och rådet (nedan kallade *budgetmyndigheten*) tillsammans med förslaget till Europeiska unionens allmänna budget.

---

[32] EGT L 317, 3.12.2001, s. 1.

8. På grundval av denna beräkning av inkomster och utgifter ska kommissionen föra in de beräkningar den anser vara nödvändiga för tjänsteförteckningen och det stödbelopp som ska belasta den allmänna budgeten i det förslaget till Europeiska unionens allmänna budget, som kommissionen ska lägga fram inför budgetmyndigheten i enlighet med artikel 314 i fördraget.

9. Budgetmyndigheten ska bevilja de anslag som utgör bidrag till byrån.

10. Budgetmyndigheten ska anta byråns tjänsteförteckning.

11. Styrelsen ska anta byråns budget tillsammans med arbetsprogrammet. Den blir slutlig när Europeiska unionens allmänna budget slutgiltigt har antagits. Styrelsen ska vid behov anpassa byråns budget och arbetsprogram till Europeiska unionens allmänna budget. Styrelsen ska utan dröjsmål vidarebefordra den till kommissionen och budgetmyndigheten.

Artikel 20
Bedrägeribekämpning

1. För bekämpning av bedrägeri, korruption och andra rättsstridiga handlingar ska Europaparlamentets och rådets förordning (EG) nr 1073/1999 av den 25 maj 1999 om utredningar som utförs av Europeiska byrån för bedrägeribekämpning (OLAF)[33] tillämpas oinskränkt.

2. Byrån ska ansluta sig till det interinstitutionella avtalet av den 25 maj 1999 mellan Europaparlamentet, Europeiska unionens råd och Europeiska gemenskapernas kommission om interna utredningar som utförs av Europeiska byrån för bedrägeribekämpning (OLAF)[34] och ska utan dröjsmål anta erforderliga bestämmelser som ska vara tillämpliga på alla anställda vid byrån.

Artikel 21
Budgetgenomförandet

1. Den verkställande direktören ska genomföra byråns budget.

2. Kommissionens internrevisor ska ha samma befogenheter gentemot byrån som gentemot kommissionens avdelningar.

3. Senast den 1 mars efter utgången av det berörda budgetåret ska kontrollorganets räkenskapsförare förse kommissionens räkenskapsförare med de preliminära räkenskaperna och en rapport om budgetförvaltningen och den ekonomiska förvaltningen under budgetåret. Kommissionens räkenskapsförare ska konsolidera institutionernas och de decentraliserade organens preliminära räkenskaper i enlighet med artikel 128 i rådets förordning (EG) nr 1605/2002 av den 25 juni 2002 med budgetförordning för Europeiska gemenskapernas allmänna budget[35] (nedan kallad *den allmänna budgetförordningen*).

4. Senast den 31 mars efter utgången av det berörda budgetåret ska kommissionens räkenskapsförare överlämna byråns preliminära redovisning till revisionsrätten tillsammans

[33] EGT L 136, 31.5.1999, s. 1.
[34] EGT L 136, 31.5.1999, s. 15.
[35] EGT L 248, 16.9.2002, s. 1.

med en rapport om budgetförvaltningen och den ekonomiska förvaltningen under budgetåret. Denna rapport om budgetförvaltningen och den ekonomiska förvaltningen under budgetåret ska också lämnas till budgetmyndigheten.

5. Efter det att revisionsrättens iakttagelser rörande byråns preliminära redovisningar som gjorts enligt bestämmelserna i artikel 129 i den allmänna budgetförordningen inkommit, ansvarar den verkställande direktören för att upprätta en slutlig redovisning av byråns räkenskaper och överlämna den till styrelsen för ett yttrande.

6. Styrelsen ska avge ett yttrande om byråns slutliga räkenskaper.

7. Den verkställande direktören ska senast den 1 juli efter varje budgetår som löpt ut, översända slutredovisningarna till Europaparlamentet, rådet, kommissionen och revisionsrätten tillsammans med yttrandet från styrelsen.

8. Den verkställande direktören ska offentliggöra slutredovisningarna.

9. Senast den 30 september ska den verkställande direktören till revisionsrätten översända ett svar på dess synpunkter. Den verkställande direktören ska också skicka detta svar till styrelsen.

10. Den verkställande direktören ska på Europaparlamentets begäran, i enlighet med artikel 146.3 i den allmänna budgetförordningen, för parlamentet lägga fram alla uppgifter som behövs för att utföra arbetet med beviljande av ansvarsfrihet för det berörda budgetåret.

11. På rekommendation av rådet ska Europaparlamentet före den 30 april år n+2 bevilja den verkställande direktören ansvarsfrihet beträffande budgetens genomförande år n.

AVSNITT 5 ALLMÄNNA BESTÄMMELSER

Artikel 22
Rättslig ställning

1. Byrån ska vara ett EU-organ. Den ska vara en juridisk person.

2. Byrån ska i varje medlemsstat ha den mest vittgående rättskapacitet som tillerkänns juridiska personer enligt den nationella lagstiftningen. Den får i synnerhet förvärva och avyttra lös och fast egendom samt föra talan inför domstolar och andra myndigheter.

3. Byrån ska företrädas av den verkställande direktören.

Artikel 23
Personal

1. De regler och föreskrifter som gäller för tjänstemän och andra anställda vid Europeiska unionen ska gälla även för byråns personal, inklusive dess verkställande direktör.

2. Styrelsen ska gentemot den verkställande direktören utöva de befogenheter som tillkommer tillsättningsmyndigheten enligt tjänsteföreskrifterna och den myndighet som har rätt att ingå avtal enligt anställningsvillkoren.

3. Den verkställande direktören ska gentemot sin personal utöva de befogenheter som tillkommer tillsättningsmyndigheten enligt tjänsteföreskrifterna och den myndighet som har rätt att ingå avtal enligt anställningsvillkoren.

4. Byrån får anställa nationella experter som är utlånade från medlemsstaterna. Byrån ska i sina interna verksamhetsregler fastställa formerna för hur detta ska genomföras i praktiken.

Artikel 24
Immunitet och privilegier

Byrån och dess personal ska omfattas av protokollet om Europeiska gemenskapernas immunitet och privilegier.

Artikel 25
Ansvar

1. Byråns avtalsrättsliga ansvar ska regleras av den lagstiftning som är tillämplig på avtalet i fråga.

Europeiska unionens domstol ska ha behörighet att döma enligt skiljedomsklausul i avtal som ingås av byrån.

2. Vad beträffar utomobligatoriskt ansvar ska byrån enligt de allmänna principer som är gemensamma för medlemsstaternas rättsordningar ersätta skada som vållats av byrån själv eller dess personal under tjänsteutövning.

Domstolen ska vara behörig att avgöra tvister som rör ersättning för sådana skador.

3. De anställdas personliga ansvar gentemot byrån ska regleras av de relevanta bestämmelser som är tillämpliga på byråns personal.

Artikel 26
Språk

1. Bestämmelserna i förordning nr 1 av den 15 april 1958 om vilka språk som ska användas i Europeiska ekonomiska gemenskapen[36] ska tillämpas på byrån. Medlemsstaterna och övriga organ som tillsatts av dem kan vända sig till byrån och har rätt att få svar på det EU-språk de väljer.

2. De översättningar som krävs för byråns verksamhet ska tillhandahållas av Översättningscentrum för Europeiska unionens organ.

[36] EGT 17, 6.10.1958, s. 385, s. 58. Förordningen senast ändrad genom 1994 års anslutningsakt.

Artikel 27
Skydd av personuppgifter

Vid behandling av uppgifter som rör enskilda ska byrån omfattas av bestämmelserna i förordning (EG) nr 45/2001.

Artikel 28
Tredjeländers deltagande

1. Byrån ska låta de länder delta som med Europeiska unionen slutit avtal enligt vilka de har antagit och tillämpar EU-lagstiftningen på det område som omfattas av denna förordning.

2. Det ska, i enlighet med tillämpliga bestämmelser i dessa avtal, fastställas främst på vilket sätt och i vilken omfattning dessa länder ska delta i byråns arbete, även de bestämmelser som gäller deltagande i de initiativ som byrån tar samt finansiella bidrag och personal.

AVSNITT 6 SLUTBESTÄMMELSER

Artikel 29
Översynsklausul

1. Inom tre år från dagen för inrättandet enligt artikel 34 ska kommissionen göra en utvärdering på grundval av den arbetsbeskrivning som antagits av styrelsen med hänsyn tagen till alla berörda intressenter. I utvärderingen ska man bedöma byråns påverkan och effektivitet i förhållande till målen enligt artikel 2 samt hur effektiva byråns arbetsmetoder är. Kommissionen ska i synnerhet göra utvärderingen för att fastställa om en byrå fortfarande är ett effektivt instrument och om byråns mandatperiod bör förlängas ytterligare utöver den period som anges i artikel 34.

2. Kommissionen ska översända utvärderingsresultatet till Europaparlamentet och rådet och de ska offentliggöras.

3. Styrelsen ska ta emot utvärderingen och utfärda rekommendationer till kommissionen om hur denna förordning och byrån och dess arbetsmetoder eventuellt bör ändras. Styrelsen och den verkställande direktören ska ta hänsyn till utvärderingen i sambands med byråns fleråriga planering.

Artikel 30
Samarbete med värdmedlemsstaten

Byråns värdmedlemsstat ska säkerställa bästa möjliga förutsättningar för en smidig och effektiv drift av byrån.

Artikel 31
Administrativ kontroll

Byråns verksamhet ska övervakas av ombudsmannen i enlighet med artikel 228 i fördraget.

Artikel 32
Upphävande och succession

1. Förordning (EG) nr 460/2004 ska upphöra att gälla.

Hänvisningar till förordning (EG) nr 460/2004 ska betraktas som hänvisningar till den här förordningen.

2. Byrån efterträder den byrå som inrättades genom förordning (EG) nr 460/2004 när det gäller all äganderätt samt alla avtal, rättsliga skyldigheter, anställningskontrakt, finansiella åtaganden och ansvarsskyldigheter.

Artikel 33
Mandatperiod

Byrån inrättas från och med […] för en femårsperiod.

Artikel 34
Ikraftträdande

Denna förordning träder i kraft dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning* och ska tillämpas från och med den 14 mars 2012 eller dagen efter det att den offentliggjorts, beroende på vad som inträffar senast.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i ... den

På Europaparlaments vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

FINANSIERINGSÖVERSIKT FÖR FÖRSLAG TILL RÄTTSAKT 1.

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets beteckning

Förslag till Europaparlamentets och rådets förordning om inrättandet av Europeiska byrån för nät- och informationssäkerhet

1.2. Politikområde(n) som berörs i den verksamhetsbaserade förvaltningen/budgeteringen[37]

Informationssamhället och medier

Regelverk för den digitala agendan

1.3. Typ av förslag eller initiativ

☐ Förslaget/initiativet rör **en ny åtgärd**

☐ Förslaget/initiativet rör **en ny åtgärd efter ett pilotprojekt/en förberedande åtgärd**[38]

☑ Befintlig åtgärd vars genomförande **förlängs i tiden**

☐ Förslaget/initiativet rör **en åtgärd som omriktas mot en ny åtgärd**

1.4. Mål

1.4.1. Fleråriga strategiska mål för kommissionen som förslaget eller initiativet är avsett att bidra till

Samstämmigt reglering– ge kommissionen och medlemsstaterna vägledning och råd om hur man ska uppdatera och utveckla ett normativt regelverk för nät- och informationssäkerhet som präglas av en helhetssyn.

Förebyggande, spårande och insatser – förbättra beredskapen genom att bidra till europeisk kapacitet för tidig varning och incidenthantering samt europeiska beredskapsplaner och övningar.

Ökning av beslutsfattarnas kunskaper – ge kommissionen och medlemsstaterna bistånd och råd för att uppnå en hög kunskapsnivå i hela EU om nät- och informationssäkerhetsfrågor. Förslaget syftar också till att ge intressenter från näringslivet information om tillämpningen. Det här innefattar även framtagande, analys och tillhandahållande av data om nät- och informationssäkerhetsöverträdelsernas ekonomi och konsekvenser, drivkrafter för intressenter att investera i nät- och informationssäkerhetsåtgärder, identifiering av risker samt indikatorer för nät- och informationssäkerhetssituationen i hela EU, etc.

---

[37] ABM: Verksamhetsbaserad förvaltning och verksamhetsbaserad budgetering benämns ibland med de interna förkortningarna ABM respektive ABB.

[38] I enlighet med artikel 49.6 a eller b i budgetförordningen.

Användarinflytande – utveckla en säkerhets- och riskhanteringskultur genom att främja informationsutbyte och ett brett samarbete mellan aktörer från offentlig och privat sektor, även till direkt gagn för medborgarna och för att utveckla en kultur av medvetenhet om nät- och informationssäkerhet.

Skydd av Europa mot internationella hot – uppnå en hög grad av samarbete med tredjeländer och internationella organisationer för att främja en gemensam global syn på nät- och informationssäkerhet och se till att internationella initiativ på hög nivå får genomslag i Europa.

Mot genomförande i samverkan – främja samverkan i genomförandet av nät- och informationssäkerhetspolitik.

Bekämpande av cyberbrottslighet – integrera nät- och informationssäkerhetsaspekter i kampen mot cyberbrottslighet i diskussioner om och utbyte av god praxis mellan offentliga och privata intressenter, i synnerhet genom samarbete med myndigheter kopplade till (f.d.) andra och tredje pelaren, t.ex. Europol.

1.4.2. Specifika mål eller verksamheter inom den verksamhetsbaserade förvaltningen och budgeteringen som berörs

Särskilt mål

Att öka nät- och informationssäkerheten, för att utveckla en kultur av nät- och informationssäkerhet till gagn för medborgare, konsumenter, företag och offentliga sektorns organisationer, samt att kartlägga utmaningar som aktualiseras genom framtidens nät och Internet.

Berörda verksamheter enligt den verksamhetsbaserade förvaltningen och budgeteringen

Politik på området för elektronisk kommunikation och nätsäkerhet

1.4.3. Verkan eller resultat som förväntas

Initiativet väntas få följande ekonomiska effekter:

- Ökad tillgång till information om dagens och morgondagens utmaningar och risker kopplade till säkerhet och motståndskraft.

- Inget dubbelarbete vid de enskilda medlemsstaternas insamling av relevant information om risker, hot och sårbara punkter.

- Beslutsfattarna bättre informerade vid beslut.

- Högre kvalitet på nät- och informationssäkerhetsbestämmelserna i medlemsstaterna tack vare spridning av bästa praxis.

- Stordriftsfördelar vid incidenthantering på EU-nivå.

- Mer investeringar främjas genom gemensamma mål och standarder för säkerhet och motståndskraft på EU-nivå.

- Lägre operativa risker för företagen tack vare högre nivå av säkerhet och motståndskraft.

- Mer sammanhängande åtgärder för att bekämpa cyberbrottslighet.

Initiativet väntas få följande sociala effekter:

- Ökat förtroende för informationssamhällets tjänster och system.

- Ökat förtroende för EU:s inre marknad genom bättre konsumentskydd.

- Ökat utbyte av information och kunskap med länder utanför EU.

- Bättre skydd av EU:s grundläggande mänskliga rättigheter genom lika nivå av skydd för EU-medborgarnas personuppgifter och personliga integritet.

De förväntade miljöeffekterna är minimiala:

- Minskade koldioxidutsläpp p.g.a. bland annat mindre resande till följd av en ökad användning av IKT-system och IKT-tjänster samt lägre elförbrukning till följd av stordriftsfördelar vid genomförandet av säkerhetskrav.

1.4.4. Indikatorer för bedömning av resultat eller verkan

Övervakningsindikatorerna per mål är följande:

Samstämmig reglering:

- Antal medlemsstater som har använt byråns rekommendationer i sin beslutsprocess.

- Antal studier som syftar till att kartlägga luckor och inkonsekvenser när det gäller standardisering inom området nät- och informationssäkerhet.

- Minskade skillnader mellan olika medlemsstaters sätt att hantera nät- och informationssäkerhet.

Förebyggande, spårande och insatser:

- Antal kurser om nätsäkerhet som anordnas.

- Tillgången till fungerande system för tidig varning vid nya risker och angrepp.

- Antal nät- och informationssäkerhetsövningar på EU-nivå som samordnas av byrån.

Ökning av beslutsfattarnas kunskaper

- Antalet studier för att samla in information om aktuella och väntade nät- och informationssäkerhetsrisker och teknik för riskförebyggande.

- Antal samråd med offentliga organ som hanterar nät- och informationssäkerhetsfrågor.

- Tillgången till en europeisk ram för att organisera insamlingen av nät- och informationssäkerhetsdata.

Användarinflytande:

- Antal identifierade goda arbetsmetoder för branschen.

- Nivån på privata intressenters investeringar i säkerhetsåtgärder.

Skydd av Europa mot internationella hot:

- Antal konferenser/möten mellan EU:s medlemsstater för att fastställa gemensamma nät- och informationssäkerhetsmål.

- Antal möten mellan europeiska och internationella nät- och informationssäkerhetsexperter.

Mot genomförande i samverkan:

- Antal utvärderingar av hur regelverket följs.

- Antal EU-omfattande nät- och informationssäkerhetsmetoder.

Bekämpande av cyberbrottslighet

- Regelbundenheten i interaktionen med f.d. andra och tredje pelarens byråer.

- Antal tillfällen då expertis tillhandahålls i brottsutredningar.

1.5. Motivering till förslaget eller initiativet

1.5.1. Behov som ska tillgodoses på kort eller lång sikt

Enisa inrättades ursprungligen 2004 för att hantera hot och eventuella brott mot nät- och informationssäkerheten. Sedan dess har nät- och informationssäkerhetsproblemen utvecklats i takt med teknikens och marknadens utveckling. De har varit föremål för reflektion och diskussioner. Därför är det nu dags för en modernisering och mer detaljerad beskrivning av de exakta problem som identifierats och hur dessa påverkas av det föränderliga nät- och informationssäkerhetslandskapet.

1.5.2. Mervärde av Europeiska unionens deltagande

Nät- och informationssäkerhetsproblem följer inte nationella gränser och kan därför inte åtgärdas på ett effektivt sätt enbart på nationell nivå. Samtidigt finns det stora skillnader i hur problemet hanteras av myndigheter i olika medlemsstater. Dessa skillnader kan utgöra ett allvarligt hinder för genomförandet av ändamålsenliga EU-mekanismer för att förbättra nät- och informationssäkerheten i Europa. Eftersom IKT-infrastrukturerna är sammankopplade till sin natur påverkas effektiviteten i åtgärder som vidtas på nationell nivå i en medlemsstat fortfarande starkt av de lägre nivåerna på åtgärder i andra medlemsstater och bristen på systematiskt gränsöverskridande samarbete. Otillräckliga nät- och informationssäkerhetsåtgärder som leder till en incident i en medlemsstat kan orsaka störningar av tjänsterna i andra medlemsstater.

Dessutom medför mångfalden av säkerhetskrav stora kostnader för företag som är verksamma på EU-nivå och en fragmentering och brist på konkurrens på EU:s inre marknad.

Beroendet av nät och informationssystem ökar och därför tycks beredskapen för incidenthantering otillräcklig.

Det finns allvarliga brister i de nuvarande nationella systemen för tidig varning och incidenthantering. Förfaranden och praxis för övervakning och rapportering av säkerhetsincidenter i nät skiljer sig mycket mellan olika medlemsstater. I en del länder är processerna inte formaliserade, medan det i andra länder saknas en behörig myndighet som kan ta emot och handlägga rapporter om incidenter. Det finns inga europeiska system. Till följd av detta kan tillhandahållandet av grundläggande nödvändigheter störas i grunden av nät- och informationssäkerhetsincidenter och ändamålsenliga reaktioner bör förberedas. I kommissionens meddelande om skydd av kritisk kommunikations- och informationsinfrastruktur betonades behovet av europeisk kapacitet för tidig varning och incidenthantering, eventuellt understödd genom Europatäckande övningar.

Det finns ett tydligt behov av policyinstrument för att aktivt identifiera nät- och informationssäkerhetsrisker och sårbara punkter, inrätta lämpliga insatsmekanismer (t.ex. genom kartläggning och spridning av god praxis) och säkerställa att intressenterna känner till och tillämpar dessa mekanismer.

1.5.3. Lärdomar från liknande åtgärder

Se punkterna *1.5.1 och 1.5.2.*

1.5.4. Förenlighet med andra finansieringsformer och eventuella synergieffekter

Det här initiativet är helt förenligt med den allmänna diskussionen om nät- och informationssäkerhet och andra initiativ som fokuserar på nät- och informationssäkerhetens framtid. Det är en av de viktigaste delarna i den digitala agendan för Europa, som är ett centralt initiativ i strategin Europa 2020.

1.6. Tid under vilken åtgärden kommer att pågå respektive påverka resursanvändningen

☑ **Begränsad**

– ☑ Startpunkten för den femåriga förlängningen kommer att vara den 14 mars 2012 eller den dag då den nya förordningen träder i kraft, beroende på vad som infaller senast.

– ☑ Finansiella konsekvenser 2012–2017

☐ **Obestämd**

– Efter en inledande period ÅÅÅÅ–ÅÅÅÅ,

– beräknas genomförandetakten nå en stabil nivå

1.7. Planerad(e) förvaltningsmetod(er)[39]

☐ **Direkt centraliserad förvaltning** inom kommissionen

☑ **Indirekt centraliserad förvaltning** genom delegering till

– ☐ genomförandeorgan

– ☑ organ som inrättats av gemenskaperna[40]

– ☐ nationella offentligrättsliga organ eller organ som anförtrotts uppgifter som faller inom offentlig förvaltning

– ☐ personer som anförtrotts ansvaret för genomförandet av särskilda åtgärder som följer av avdelning V i fördraget om Europeiska unionen och som anges i den grundläggande rättsakten i den mening som avses i artikel 49 i budgetförordningen

☐ **Delad förvaltning** med medlemsstaterna.

☐ **Decentraliserad förvaltning** tillsammans med tredjeländer

☐ **Gemensam förvaltning** tillsammans med internationella organisationer (*ännu ej fastställt*)

[39] Närmare förklaringar av de olika metoderna för genomförande med hänvisningar till respektive bestämmelser i budgetförordningen återfinns på BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[40] I enlighet med artikel 185 i budgetförordningen.

2. FÖRVALTNING

2.1. Bestämmelser om uppföljning och rapportering

Byråns verkställande direktör ansvarar för övervakning och utvärdering av att byråns arbete följer de angivna målen och ska rapportera årligen till styrelsen.

Den verkställande direktören ska sammanställa en allmän rapport som omfattar all verksamhet som bedrivits av byrån under året och i rapporten ska ingå en avstämning av de resultat som uppnåtts i förhållande till målen i det årliga arbetsprogrammet. När byråns allmänna rapport har antagits av styrelsen ska den verkställande direktören vidarebefordra denna till Europaparlamentet, rådet, kommissionen, revisionsrätten, Europeiska ekonomiska och sociala kommittén och Regionkommittén, samt låta offentliggöra denna.

2.2. Administrations- och kontrollsystem

2.2.1. Identifierad(e) risk(er)

Sedan Enisa inrättades 2004 har byråns verksamhet utvärderats både internt och externt.

I enlighet med artikel 25 i Enisa-förordningen inleddes utvärderingsarbetet 2006/2007 genom en oberoende utvärdering som gjordes av en extern expertgrupp. Den externa expertgruppens rapport[41] visade att de politiska grundtankar som låg till grund för inrättandet av byrån och för dess målsättningar fortfarande var giltiga och rapporten pekade också på ett antal problem som behövde åtgärdas.

I mars 2007 underrättade kommissionen styrelsen om utvärderingen och styrelsen utfärdade därefter egna rekommendationer för byråns framtid och föreslog ändringar av Enisa-förordningen[42].

I juni 2007 lade kommissionen fram sin egen bedömning av resultaten av den externa utvärderingen och styrelsens rekommendationer i form av ett meddelande till Europaparlamentet och rådet[43]. I meddelandet anges att det är nödvändigt att besluta om byråns mandat ska förlängas eller om den ska ersättas av en annan mekanism, som ett permanent forum för intressenter eller ett nätverk av organisationer på säkerhetsområdet. Genom meddelandet inleddes också ett offentligt samråd i frågan. Syftet var att med hjälp av ett antal frågor stimulera till diskussion och få in synpunkter från berörda aktörer i EU[44].

2.2.2. Planerad(e) kontrollmetod(er)

Se ovan punkt 2,1 och punkt 2.2.1.

---

41 http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm.

42 I enlighet med artikel 25 i Enisa-förordningen. Det dokument som antogs av byråns styrelse, som också innehåller styrelsen reflektioner, kan läsas i sin helhet på följande webbplats: http://enisa.europa.eu/pages/03_02.htm.

43 Meddelande från kommissionen till Europaparlamentet och rådet om utvärderingen av den europeiska byrån för nät- och informationssäkerhet (Enisa), KOM(2007)285 slutlig, 1.6.2007. Meddelandet finns på följande webbplats: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:EN:NOT.

44 http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=EnisaFuture&lang=en.

2.3. Åtgärder för att förebygga bedrägeri och oegentligheter/oriktigheter

Betalningen för beställda tjänster eller undersökningar ska kontrolleras av byrån innan utbetalningen görs, med beaktande av villkoren i avtalen, ekonomiska principer samt god ekonomisk och administrativ sed. Åtgärder för bedrägeribekämpning (övervakning, rapporteringskrav osv.) kommer att ingå i alla avtal och kontrakt mellan byrån och dess betalningsmottagare.

3. BERÄKNAD FINANSIELL PÅVERKAN AV FÖRSLAGET/INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

- Befintliga budgetrubriker i utgiftsdelen

Rubrik i den fleråriga budgetramen	Budgetrubrik	Typ av utgifter	Bidrag			
	Antal / beskrivning	Diff. anslag/Icke-diff. anslag (45)	Från Efta-länder[46]	från kandidat-länder[47]	från tredje-länder	enligt artikel 18.1 aa i budgetförordningen
1a Konkurrenskraft för tillväxt och sysselsättning	09 02 03 01 Europeiska byrån för nät- och informationssäkerhet – Bidrag enligt avdelningarna 1 och 2	Diff. anslag	JA	NEJ	NEJ	NEJ
	09 02 03 02 Europeiska byrån för nät- och informationssäkerhet – Bidrag enligt avdelning 3	Diff. anslag	JA	NEJ	NEJ	NEJ
5 Administrativa utgifter	09 01 01 Utgifter för personal i aktiv tjänst inom politikområdet informationssamhället och medierna	Icke-diff. anslag	NEJ	NEJ	NEJ	NEJ
	09 01 02 11 Andra administrativa utgifter	Icke-diff. anslag	NEJ	NEJ	NEJ	NEJ

* Förslagets beräknade finansiella konsekvenser för perioden efter den nuvarande finansiella programperioden 2007–2013 täcks inte av denna finansieringsöversikt för rättsakt. På grundval av kommissionens förslag till förordning om flerårig budgetram för perioden efter 2013 och med beaktande av slutsatserna från konsekvensanalysen, kommer kommissionen att lägga fram en ändrad finansieringsöversikt för rättsakt.

45 DA = Differentierade anslag / DNA = Icke-differentierade anslag.

46 Efta: Europeiska frihandelssammanslutningen.

47 Kandidatländer och i förekommande fall potentiella kandidatländer i västra Balkan.

3.2. Beräknad påverkan på utgifter

3.2.1. Sammanfattning av den beräknade påverkan på utgifterna

Miljoner euro (avrundat till tre decimaler)

Rubrik i den fleråriga budgetramen	1.a	Konkurrenskraft för tillväxt och sysselsättning

Enisa			1 jan–13 mars 2012	14 mars–31 dec 2012	2013	2014	2015	2016	1 jan–13 mars 2017	**TOTALT 14 mars 2012 – 13 mars 2017**
Driftsanslag										
09 02 03 02 Europeiska byrån för nät- och informationssäkerhet – Bidrag enligt avdelning 3	Åtagandebemyndiganden	(1)	0,454	1,976	2,470	--	--	--	--	--
	Betalningsbemyndiganden	(2)	0,454	1,976	2,470	--	--	--	--	--
Administrativa anslag										
09 02 03 01 Europeiska byrån för nät- och informationssäkerhet – Bidrag enligt avdelningarna 1 och 2		(3)	1,293	4,697	6,120	--	--	--	--	--
TOTALT anslag under RUBRIK 1a	Åtagandebemyndiganden	=1 +3	1,747	6,673	8,590	--	--	--	--	--
	Betalningsbemyndiganden	=2+3	1,747	6,673	8,590	--	--	--	--	--

TOTALT driftsanslag	Åtagandebemy	(4)	0,454	1,976	2,470	--	--	--	--	--

	ndiganden									
	Betalningsbemyndiganden	(5)	0,454	1,976	2,470	--	--	--	--	--
TOTALT administrativa anslag som finansieras genom ramanslagen för vissa program		(6)	1,293	4,697	6,120	--	--	--	--	--
TOTALT anslag under RUBRIK 1.a i den fleråriga budgetramen	Åtagandebemyndiganden	=4+6	1,747	6,673	8,590	--	--	--	--	--
	Betalningsbemyndiganden	=5+6	1,747	6,673	8,590	--	--	--	--	--

Miljoner euro (avrundat till tre decimaler)

Rubrik i den fleråriga budgetramen	5	Administrativa utgifter

		1 jan–13 mars 2012	14 mars–31 dec 2012	2013	2014	2015	2016	1 jan–13 mars 2017	Totalt
Personal		0,085	0,342	0,427	--	--	--	--	--
Övriga administrativa utgifter		0,002	0,013	0,015	--	--	--	--	--
TOTALT GD INFSO	Anslag	0,087	0,355	0,442	--	--	--	--	--

TOTALT anslag under RUBRIK 5 i den fleråriga budgetramen	(Totalt åtagandebemyndiganden = Totalt betalningsbemyndiganden)	0,087	0,355	0,442	--	--	--	--	--

		1 jan–13 mars 2012	14 mars–31 dec 2012	2013	2014	2015	2016	1 jan–13 mars 2017	Totalt
TOTALT anslag under RUBRIKERNA 1–5 i den fleråriga budgetramen	Åtagandebemyndiganden	1,834	7,028	9,032	--	--	--	--	--
	Betalningsbemyndiganden	1,834	7,028	9,032	--	--	--	--	--

3.2.2. Beräknad påverkan på driftsanslagen

– ☐ Förslaget/initiativet kräver inte att driftsanslag tas i anspråk

– ☑ Förslaget/initiativet kräver att driftsanslag tas i anspråk enligt följande:

Åtagandebemyndiganden i miljoner euro (avrundat till tre decimaler)

Åtgärds- och resultatbeteckning ⇩	1 jan–13 mars 2012	14 mars–31 dec 2012	2013	2014	2015	2016	1 jan–13 mars 2017	**TOTALT 14 mars 2012 – 13 mars 2017**
Samstämmig reglering:	0,114	0,494	0,620	--	--	--	--	--
Förebyggande, spårande och insatser:	0,114	0,494	0,620	--	--	--	--	--
Ökning av beslutsfattarnas kunskaper	0,068	0,297	0,370	--	--	--	--	--
Användarinflytande:	0,050	0,218	0,270	--	--	--	--	--
Skydd av Europa mot internationella hot:	0,023	0,099	0,120	--	--	--	--	--
Mot genomförande i samverkan:	0,064	0,276	0,340	--	--	--	--	--
Bekämpande av cyberbrottslighet	0,023	0,098	0,120	--	--	--	--	--
TOTALT KOSTNADER	0,454	1,976	2,460	--	--	--	--	--

3.2.3. Beräknad påverkan på anslag av administrativ karaktär[48]

3.2.3.1. Sammanfattning

– ☐ Förslaget/initiativet kräver inte att administrativa anslag tas i anspråk

– ☑ Förslaget/initiativet kräver att administrativa anslag tas i anspråk enligt följande:

a) Administrativa utgifter under budgetrubrik 5 i den fleråriga budgetramen

Miljoner euro (avrundat till tre decimaler)

RUBRIK 5 i den fleråriga budgetramen	1 jan–13 mars 2012	14 mars–31 dec 2012	2013	2014	2015	2016	1 jan–13 mars 2017	**Totalt 14 mars 2012 – 13 mars 2017**
Personal	0,085	0,342	0,427	--	--	--	--	--
Övriga administrativa utgifter	0,002	0,013	0,015	--	--	--	--	--
TOTALT	0,087	0,355	0,442	--	--	--	--	--

b) Administrativa utgifter för Enisa – omfattas av budgetrubrik ”09 02 03 01 Europeisk nät- och informationssäkerhet: Rubrik 1 – Personal och rubrik 2 – Byråns drift”.

Miljoner euro (avrundat till tre decimaler)

	1 jan–13 mars 2012	14 mars–31 dec 2012	2013	2014	2015	2016	1 jan–13 mars 2017	**Totalt 14 mars 2012 – 13 mars 2017**
Personalresurser - Rubrik 1 – Personal	1,153	4,329	5,607	--	--	--	--	--
Övriga utgifter Av administrativ karaktär – Rubrik 2 – – Byråns drift”	0,140	0,368	0,513	--	--	--	--	--
TOTALT	**1,293**	**4,697**	**6,120**	--	--	--	--	--

[48] Bilagan till finansieringsöversikten är inte ifylld eftersom den inte är tillämplig på detta förslag.

3.2.3.2. Beräknat personalbehov

Varje år ska byråns tjänsteförteckning förklaras och motiveras i ett dokument kallat Personalplan som ska lämnas till budgetmyndigheten.

– ☐ Förslaget/initiativet kräver inte att personalresurser tas i anspråk

– ☑ Förslaget/initiativet kräver att personalresurser tas i anspråk enligt följande:

a) Personalresurser inom kommissionen

	1 jan–13 mars 2012	14 mars–31 dec 2012	2013	2014	2015	2016	1 jan–13 mars 2017
Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)							
XX 01 01 01 (Huvudkontoret och kommissionens representationskontor)	3,5	3,5	3,5	--	--	--	--
TOTALT	**3,5**	**3,5**	**3,5**	--	--	--	--

b) Enisas personalresurser

		1 jan–13 mars 2012	14 mars–31 dec 2012	2013	2014	2015	2016	1 jan–13 mars 2017
Enisas tjänsteförteckning (uttryckt i heltidsekvivalenter)								
Tjänstemän eller tillfälligt anställda	AD	29	31	31	--	--	--	--
	AST	15	16	16	--	--	--	--
TOTALT tjänstemän eller tillfälligt anställda		44	47	47	--	--	--	--
Övrig personal (i heltidsekvivalenter)								
Kontraktsanställda		13	14	14	--	--	--	--
Utlånade nationella experter		5	5	5	--	--	--	--
Totalt övrig personal		18	19	19	--	--	--	--
TOTALT		**62**	**66**	**66**	--	--	--	--

Beskrivning av de uppgifter som ska utföras av byråns personal:

Tjänstemän och tillfälligt	Byrån kommer att fortsätta att

anställda	– ha rådgivande och samordnade funktioner som innebär att den ska **samla in och analysera uppgifter** om informationssäkerhet. I dag samlar både offentliga och privata organisationer av olika skäl in data om IT-problem och andra uppgifter som rör informationssäkerhet. Det finns emellertid ingen central enhet på europeisk nivå som på ett övergripande sätt kan samla in och analysera data samt yttra sig och ge råd för att stödja EU:s politiska arbete inom området nät- och informationssäkerhet, – **tjäna** som ett **kompetenscentrum** dit både medlemsstaterna och EU-institutionerna ska kunna vända sig dit för att **erhålla yttranden och råd om tekniska frågor** som rör säkerhet, – bidra till ett **brett samarbete mellan olika aktörer** inom informationssamhällets område genom att t.ex. stödja uppföljningsåtgärder till stöd för säkra e-företag. Ett sådant samarbete kommer att vara en förutsättning för att de europeiska näten och informationssystemen ska fungera på ett säkert sätt. Alla berörda parter måste delta och engagera sig, – bidra till en samordnad strategi för informationssäkerhet genom att erbjuda **medlemsstaterna stöd** när det gäller t.ex. **främjande av riskbedömning** och medvetandehöjande åtgärder, – säkerställa **interoperabiliteten för nät och informationssystem** när medlemsstaterna **tillämpar** tekniska krav som påverkar säkerheten, – kartlägga **relevanta standardiseringsbehov**, bedöma befintliga säkerhetsstandarder och certifieringssystem och verka för att dessa i så stor utsträckning som möjligt används till stöd för EU-lagstiftningen, och – stödja **det internationella samarbetet** inom detta område, vilket blir allt viktigare med tanke på att nät- och informationssäkerhetsfrågor är globala.
Extern personal	Se ovan

3.2.4. Förenlighet med den gällande fleråriga budgetramen

– ☑ Förslaget/initiativet är förenligt med den gällande fleråriga budgetramen.

– ☐ Förslaget/initiativet kräver omfördelningar under den berörda rubriken i den fleråriga budgetramen.

– ☐ Förslaget/initiativet kräver tillämpning av flexibilitetsinstrumentet eller revidering av den fleråriga budgetramen[49].

EU-finansieringen efter 2013 kommer att granskas i samband med en kommissionsomfattande diskussion om alla förslag för perioden efter 2013. Det här betyder att kommissionen när den lagt fram sitt förslag för nästa fleråriga budgetram kommer att lägga fram en ändrad finansieringsöversikt för rättsakt som beaktar slutsatserna från konsekvensanalysen.

3.2.5. Bidrag från tredje part

– ☐ Det ingår inga bidrag från tredje part i det aktuella förslaget eller initiativet

– ☑ Förslaget eller initiativet kommer att medfinansieras enligt följande:

Preliminära anslag i milj. euro (avrundat till tre decimaler)

	1 jan–13 mars 2012	14 mars–31 dec 2012	2013	2014	2015	2016	1 jan–13 mars 2017	**Totalt 14 mars 2012 – 13 mars 2017**
Efta	0,042	0,160	0,206	--	--	--	--	--

3.3. Beräknad påverkan på inkomsterna

– ☑ Förslaget/initiativet påverkar inte budgetens inkomstsida.

– ☐ Förslaget/initiativet påverkar inkomsterna på följande sätt:

– ☐ Påverkan på egna medel

– ☐ Påverkan på ”diverse inkomster”

[49] Se punkterna 19 och 24 i det interinstitutionella avtalet.