*Justitiedepartementet*
*103 33 Stockholm*
*ju.registrator@regeringskansliet.se*

# Yttrande över SOU 2015:23 Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten

Ekobrottsmyndigheten lämnar härmed sitt yttrande över rubricerat betänkande.

## Sammanfattning

Informations- och cybersäkerheten i Sverige behöver stärkas. Ekobrottsmyndigheten stödjer därför inrättandet av en nationell strategi för statens informations- och cybersäkerhet.

Ekobrottsmyndigheten har dock synpunkter på flera av de förslag till åtgärder som ingår i denna strategi. I många fall är myndighetens ställningstagande beroende av hur åtgärderna ska införas i praktiken.

Vidare är några av förslagen så övergripande beskrivna att de är svåra att bedöma. Detta gäller bland annat myndighetsrådet, den nationella styrmodellen och kravet på incidentrapportering.

Ekobrottsmyndigheten är starkt kritisk till förslaget om införande av sensorsystem i sin nuvarande utformning, då de rättsliga och integritetsmässiga konsekvenserna inte är närmare belysta eller analyserade.

Ekobrottsmyndigheten anser det vara angeläget att knyta an vissa viktiga frågor till det som i betänkandet sägs om brottsbekämpning och då i synnerhet om tvångsmedel i den digitala miljön.

Ekobrottsmyndigheten menar att utredningens författningsförslag bör genomgå vissa förändringar och eventuellt ges förnyad beredning och remissbehandling innan det kan ligga till grund för beslut. En större samordning mellan utredningens författningsförslag och förslaget till ny säkerhetsskyddslag vore också av godo.

När det gäller konsekvensanalysen delas uppfattningen att vissa av förslagen kan rymmas inom myndigheternas befintliga budget, men samtidigt anser vi att denna samlade ambitionshöjning ofrånkomligen kommer att medföra ett ökat resursbehov för de enskilda myndigheterna (även om behovet blir störst hos MSB), vilket inte framgår tillräckligt.

## Övergripande synpunkter

Informations- och cybersäkerheten i Sverige behöver stärkas och Ekobrottsmyndigheten ser positivt på strategin och de flesta förslagen inom denna. I många fall är dock myndighetens ställningstaganden beroende av hur förslagen ska införas i praktiken.

Ekobrottsmyndigheten saknar tillräcklig analys och motivering kring flera av förslagen. I de fall där en åtgärd är ytterst övergripande beskriven är det svårt att med säkerhet förstå åtgärdens omfattning och konsekvenser både för myndigheten och för informationssäkerheten på nationell nivå. Enligt Ekobrottsmyndigheten behövs det tydliga förarbeten till så viktiga förordningar som här föreslås.

En generell synpunkt är att förslagen både teoretiskt och praktiskt måste fungera i samspel med andra författningskrav och aktuella förslag i inom angränsande områden. Detta avser inte minst SOU 2015:25 En ny säkerhetsskyddslag samt MSB:s föreslagna föreskrifter för statliga myndigheters informationssäkerhet (som ska ersätta nuvarande MSBFS 2009:10). Ekobrottsmyndighetens uppfattning är att utredningen har brister här alternativt att samspelet inte är tillräckligt tydligt beskrivet i betänkandet.

Motsvarande gäller för samordningen med de områden för informationshantering där Riksarkivet har föreskriftsrätt. De krav på redovisning av informationsflöden som blir konsekvensen av den föreslagna lagstiftningen bör tydligare samordnas med de krav som finns i Riksarkivets föreskrifter om arkivredovisning (RA-FS 2008:4). Att integrera kraven borde i sig inte vara problematiskt och Ekobrottsmyndigheten anser det vara av största vikt att så sker.

Om alla delar av regleringen av informationshantering korresponderar med varandra underlättar det myndighetens arbete med att ta fram för området relevanta styrdokument. Blir det praktiska utfallet av den sammanlagda regleringen på informationshanteringsområdet att myndigheten måste hålla sig med ett flertal separata styrdokument för informationshantering i form av dokumenthanteringsplaner, policydokument, informationsflödesredovisningar och liknande ökar riskerna för att det enskilda styrdokumentets genomslagskraft i verksamheten blir bristfällig. Den övergripande målsättningen bör därför vara att lagstiftningen utformas på ett sådant sätt att det totala antalet styrdokument för informationshantering som blir utfallet hålls nere och i möjligaste mån går att sammanfoga eller på ett enkelt och begripligt sätt samordna.

En synpunkt som återkommer i samband med flera åtgärder gäller behovet av analys kring sekretessfrågor i samband med åtgärden. Ekobrottsmyndigheten vill också betona det utökade behovet av praktiskt stöd inom området som de ambitionshöjande förslagen medför. Detta behov får inte underskattas och myndigheten menar att utredningen tydligare borde lyft fram frågor om hur statliga myndigheter kan få stöd inom informationssäkerhet. Exempelvis borde de stöduppdrag som MSB ska ha varit tydligare beskrivna.

## Avsnitt 9.1 En nationell strategi för statens informations- och cybersäkerhet, sidan 203

Ekobrottsmyndigheten stödjer inrättandet en nationell strategi för statens informations- och cybersäkerhet men har synpunkter på flera av de förslag till åtgärder som ingår i den föreslagna strategin.

### 9.1.4 Strategins innehåll, sidan 208

Enligt utredningen bör en strategi för statens informations- och cybersäkerhet ha ett medellångt perspektiv som kan ligga till grund för åtgärder på två till tre års sikt. Det kan ifrågasättas om detta inte är ett väl kort perspektiv. De åtgärder som föreslås behöver i flera fall betydligt längre tid för att få effekt. Det är viktigt att arbeta långsiktigt med informationssäkerhet utan att man för den skull ger avkall på snabbt och effektivt agerande utifrån signaler ifrån verksamhet och omvärldsbevakning.

## Avsnitt 9.2 Ansvar, styrning, samordning och tillsyn, sidan 211

### 9.2.1 En nationell styrmodell, sidan 211

Ekobrottsmyndigheten kan med utredningens underlag inte bedöma nytta, effekt eller kostnad för Ekobrottsmyndigheten om förslaget med en nationell styrmodell skulle genomföras.

Förslaget saknar en djupare beskrivning över vad gemensamma skyddsnivåer, kravbilder, metoder betyder konkret, hur verksamhetsbehov och skillnader mellan myndigheternas verksamhet påverkar förslaget samt hur förslaget skiljer sig från MSB nu gällande föreskrift om ledningssystem för informationssäkerhet.

Styrmodellens utformning bör konkretiseras innan förslaget genomförs.

### 9.2.2 Inrättande av ett myndighetsråd, sidan 215

Ekobrottsmyndigheten stödjer synen på att samverkan är viktigt för informationssäkerhets-arbetet. Myndighetsrådets uppgifter beskrivs dock som mer omfattande än samverkan. Uppgiften att förebygga, följa och åtgärda brister i statens informationssäkerhet samt mandatet att förvalta och utveckla tillämpliga krav på standarder och certifiering för produkter och tjänster med bäring på informationssäkerhet i samhällsviktig verksamhet är mer långtgående än ett samverkansuppdrag.

Uppgifter som att vara remissinstans och samrådsforum för utveckling av den nationella styrmodellen, genomförare av strategi samt förvalta och utveckla krav ger myndighetsrådet en stor påverkan samtidigt som det anges att myndighetsrådet enbart ska inkludera relevanta myndigheter. Ekobrottsmyndigheten är frågande till vilken insyn eller påverkansmöjlighet övriga myndigheter kommer att få i detta viktiga arbete.

### 9.2.3 En ny förordning för statliga myndigheters informationssäkerhet, sidan 220

Ekobrottsmyndigheten stödjer förslaget att en ny förordning ska styra statliga myndigheters informationssäkerhet. Ekobrottsmyndigheten har dock flera synpunkter som avser ett antal föreslagna bestämmelser i en ny förordning.

**Inledande bestämmelser (1–3 §§)**

Ekobrottsmyndigheten saknar i författningsförslaget en formulering om det ansvar för stöd till statliga myndigheter som Myndigheten för samhällsskydd och beredskap ska ha.

Ekobrottsmyndigheten håller inte med om att Regeringskansliet ska undantas. Det rimmar illa med behovet av generell höjning av informationssäkerheten och bättre samordning i staten där regeringskansliet har en nyckelroll.

**Definitioner (4 §)**

Ekobrottsmyndigheten avstyrker författningsförslaget om en för staten speciell definition av begreppet informationssäkerhet. När det gäller grundläggande begrepp som används i hela samhället är det av största vikt att statsförvaltningen beaktar nationell och internationell standard för informationssäkerhet. Myndigheten anser att avvikande begreppsdefinitioner försvårar förståelsen och skapar onödiga kostnader. Myndigheten förordar att om förmåga eller spårbarhet ska betonas i samband med någon av förordningens bestämmelser bör detta i stället anges i respektive bestämmelse.

I utredningens författningsförslag förekommer flera odefinierade begrepp, exempelvis god säkerhetskultur, informationsprocesser, it-incidenter, säkra kryptografiska funktioner och säkra it-produkter. Ska dessa begrepp användas i förordningstext bör de vara tydligt definierade.

**Regler rörande det interna säkerhetsarbetet (5–10 §§)**

**5 §**

Författningsförslagets 5 § andra meningen är ett allt för vagt formulerat krav angående att beakta ledningssystem jämfört med det utredningen skriver på sidan 208 om åtgärder inom strategins första mål. Ekobrottsmyndigheten föreslår därför följande alternativa formulering. *Myndigheten ska ha ett ledningssystem som omfattar informationssäkerhet och särskilt beakta etablerade standarder för informationssäkerhet.* En sådan formulering är tydligare samtidigt som den möjliggör för en myndighet att integrera ledningssystem på ett lämpligt sätt.

**6 §**

Författningsförslagets 6 § första meningen är mer långtgående än kraven i aktuell ledningssystemstandard och förefaller oproportionerlig med hänsyn till vissa myndigheters organisation. Utredningen saknar motivering till meningens formulering. Ekobrottsmyndigheten avstyrker därför förslaget och föreslår en alternativ formulering. *Myndighetens ledning ska tydligt visa ledarskap och åtagande i fråga om informationssäkerhet*.

I författningsförslagets 6 § sista meningen används begreppet god säkerhetskultur utan någon definition. Det begreppet är attraktivt, men det kräver mer än utbildning och övning samtidigt som det går långt utanför informationssäkerhetsområdet. Om förordningen alls ska nämna kultur i detta sammanhang föreslår Ekobrottsmyndigheten följande alternativa formulering. *Myndigheten ska aktivt, genom utbildning, övning och ledarskap, verka för att en kultur etableras i organisationen där medvetenhet om informationssäkerhet ingår.*

**7 §**
Författningsförslagets 7 § första meningen anger att myndigheten ska kartlägga sina informationsprocesser. Ekobrottsmyndigheten uppfattar kravet på en viss arbetsmetod som omotiverat och det odefinierade begreppet ”informationsprocesser” som mångtydigt. Ekobrottsmyndigheten avstyrker därför författningskravet om kartläggning.

Författningsförslagets 7 § andra meningen om incidenter bör brytas ut till en egen paragraf. I meningen används det odefinierade begreppet it-incidenter. Begreppet it-incidenter kan misstolkas till att endast avse tillgänglighetsincidenter. Ekobrottsmyndigheten föreslår att svensk och internationell standard beaktas, och att begreppet informationssäkerhetsincidenter används istället.

Ekobrottsmyndigheten avstyrker författningsförslagets 7 § sista meningen om att gemensamma krav- och skyddsnivåer ska användas eftersom den frågan inte bedöms vara mogen för förordningsreglering. Myndigheten anser att innan en för myndigheterna så ingripande reglering införs bör nivåer utarbetas och provas på frivillig väg. Se vidare synpunkter angående nationell styrmodell ovan.

**8 §**
Författningsförslagets 8 § avstyrks. Texten behöver beredas ytterligare då den är svår att tolka och att tillämpa för myndigheterna. Exempelvis används det odefinierade begreppet säkra it-produkter samtidigt som svenska myndigheter idag i allt större utsträckning anskaffar it som tjänster och inte som hårdvaruprodukter. Ett annat exempel är att formuleringen av den sista meningen inte förefaller helt förenlig med upphandlingslagstiftningen.

**9 §**
Författningsförslagets 9 § 1 st bör beredas ytterligare för större tydlighet. Ekobrottsmyndigheten föreslår att orden *i en årlig plan* utgår och att stycket inleds med *Myndigheten ska årligen följa upp…*

**10 §**
Enligt Ekobrottsmyndighetens uppfattning bör författningsförslagets 10 § beredas ytterligare och kraven på värdmyndigheter förtydligas och skärpas.

**Särskilda krav på informationssäkerhetsarbete (11 §)**
**11 §**
I författningsförslagets 11 § åläggs vissa myndigheter att uppfylla särskilda krav på informationssäkerhet.

Första strecksatsen kan bli kostnadsdrivande, Ekobrottsmyndighetens kommentarer återfinns i avsnitt Statliga nätverk nedan.

Ekobrottsmyndigheten avstyrker den andra strecksatsen eftersom användningen av dessa sensorsystem och de rättsliga och integritetsmässiga konsekvenserna inte är närmare belysta eller analyserade. Motiveringar återfinns i avsnitt angående Statliga nätverk nedan. Ekobrottsmyndigheten anser att den tredje strecksatsen bör beredas ytterligare. Myndigheten menar att krav på informationssäkerhetskompetens hos de viktigaste myndigheterna inte ska fokuseras på en enda person eller roll.

**Säkra kryptografiska funktioner (12–14 §§)**
Ekobrottsmyndigheten anser att definitionen av säkra kryptografiska funktioner i krisberedskapsförordningen (2006:942) ska flyttas med om dessa regler flyttas till en ny förordning.

**Upphandling av it-system och it-produkter (15–16 §§)**
**15 §**
Författningsförslagets 15 § 4 st behöver beredas ytterligare. Stycket synes inte överensstämma inte med 10 kap. 2 § offentlighets- och sekretesslagen (2009:400). Författningsförslagets ordval *ska endast* bör ersättas med *får endast*. Här som i förordningen i sin helhet bör begreppet it-incidenter bytas ut.

**16 §**
Författningsförslagets 16 § är både svårtolkad och oproportionerligt kostnadsdrivande då samhällsviktig verksamhet utgör en omfattande del av de statliga myndigheternas verksamhet. Texten behöver beredas ytterligare då den är svår att tolka och att tillämpa för myndigheterna. Exempelvis används det odefinierade begreppet säkra och certifierade it-produkter samtidigt som svenska myndigheter idag i allt större utsträckning anskaffar it som tjänster istället för som hårdvaruprodukter. Ett annat exempel är att formuleringen av den sista meningen inte förefaller helt förenlig med upphandlingslagstiftningen.

**It-incidentrapportering (17 §)**

**17 §**
Ekobrottsmyndigheten ser behovet av en obligatorisk incidentrapportering för vissa allvarliga incidenter. Trots att frågan utretts tidigare är det dock Ekobrottsmyndighetens bedömning att det fortfarande saknas vissa nödvändiga förutsättningar för ett införande via förordning. Viktiga förutsättningar är förutom tekniska stödsystem och tillräckliga resurser även möjligheter att med sekretess skydda tekniska uppgifter och personuppgifter som kan förekomma både i incidentrapporterna och i den returinformation som den rapporterande myndigheten behöver få tillgång till. Motiveringar återfinns i avsnittet Incidentrapportering nedan.

**Tillsyn, föreskrifter, Myndighetsrådets uppgifter (18–20 §§)**
**18 §**
Ekobrottsmyndighetens synpunkter framgår av avsnitt om Inrättande av ett myndighetsråd ovan.

**19 §**
Ekobrottsmyndigheten avstyrker författningsförslaget i denna del. Se avsnitt om Tillsyn nedan för motivering och alternativa förslag.

**20 §**
Författningsförslagets första och fjärde bemyndiganden är mycket långtgående. Författningsförslagets tredje bemyndigande är svårtolkat vilket Ekobrottsmyndigheten påpekat angående 16 § ovan.

### 9.2.4 Tillsyn, sidan 227
Ekobrottsmyndigheten stödjer att tillsynen inom informationssäkerhetsområdet bör samordnas och förstärkas. Myndigheten delar dock inte utredarens syn att den bästa lösningen är att MSB utöver sina styrande och stödjande roller även bör ges rollen att utöva tillsyn inom området.

Ekobrottsmyndigheten vill påpeka följande svagheter i en sådan lösning. Det förslag till ny säkerhetsskyddslag som nu remissbehandlas föreslår att säkerhetsskyddslagen ges en delvis bredare tillämpning. Därmed skulle en förstärkt tillsyn innebära en ökad belastning och risk för dubbelarbete för många myndigheter som blir föremål för överlappande tillsyn från både Säkerhetspolisen och MSB inom informationssäkerhet. Det kan även tänkas att tillsyn från MSB i vissa fall kan hindras av sekretess med hänsyn till säkerhetsskydd och Sveriges säkerhet. En svaghet med förslaget är att den stödjande roll som MSB har kan försvagas om både den styrande rollen förstärks och en ny tillsynsroll tillkommer. Detta kan ske om MSB stegvis skulle anpassa sitt stöd utefter de nya uppdragen med utökad styrning och tillsyn. Detta skulle sannolikt orsaka en negativ effekt på informationssäkerhetsarbetet inom statsförvaltningen då det inte finns någon annan myndighet som stödjer myndigheterna i samma omfattning. Betänkandet ger inte heller stöd för att övriga förslag skulle kompensera för effekten av uppdraget med tillsyn.

## Avsnitt 9.3 Staten som tydlig kravställare, sidan 235

### 9.3.1 Kravställning vid upphandling, sidan 236
Ekobrottsmyndigheten stödjer generellt en bättre kravställning av säkerhet vid upphandling. Statliga myndigheter har en allt mer omfattande behandling av information med stöd av IT. En utveckling mot större andel tjänsteupphandlingar är påtaglig. Ekobrottsmyndigheten ser utmaningar i att utforma regler och krav vid upphandling som står i samklang med upphandlingslagstiftningen. Detta påpekades även i synpunkter på författningsförslaget ovan.

Ekobrottsmyndigheten ser det som bekymmersamt att utredningen inte har konkretiserat vad av detta stora produkt- och tjänsteområde som ska regleras med stöd av standarder och certifieringar. Detta då betänkandet anger att vanligt förekommande it-produkter ska inkluderas. Ekobrottsmyndigheten har på denna grund inte i detalj kunnat bedöma eventuella konsekvenser i form av nytta och kostnader av förslaget även om det står klart att det på kort sikt är kostnadsdrivande. De allvarligaste konsekvenserna kan uppstå om styrande regler tvingar vissa myndigheter att avropa certifierade säkra produkter. Skulle det innebära att Ekobrottsmyndigheten inte längre kan nyttja etablerade produkter på marknaden kan det få allvarliga konsekvenser för it-verksamheten. Den certifierade produktfloran är idag klart begränsad och myndigheterna får utmaningar med kompetensförsörjning kring sådana produkter då dessa idag i första hand används inom försvaret.

Förslag om att det bör införas krav för att rapportera vilken leverantör som valts då avrop sker från ramavtal innebär inga större konsekvenser för Ekobrottsmyndigheten. Ekobrottsmyndigheten vill dock framhålla att ett sådant förslag endast ger en förbättrad lägesbild över eventuella sårbarheter. Hur sårbarheten eller risken ska minskas berörs inte i betänkandet. Om en sådan bestämmelse ska införas bör dess syfte och mål vara tydligt beskrivna i förarbetet så att också den tänkta effekten av förslaget kan bedömas.

## Avsnitt 9.4 Säkrare kommunikation i staten, sidan 246

### 9.4.1 Statliga nätverk, sidan 246

Ekobrottsmyndigheten lämnar synpunkter på utredningens samtliga förslag i denna del.

**Utvecklade kommunikationssystem för säkrare kommunikation i staten, sidan 248**

Ekobrottsmyndigheten stödjer förslaget att samtliga myndigheter i bilagan till KBF ansluter sig till SGSI. Ekobrottsmyndigheten vill även föreslå att MSB ges ett helhetsansvar för ackrediteringen till SGSI för att kunna vara effektiv vid en utökning av anslutna myndigheter.

Som nämnts ovan kan författningsförslagets 11 § första strecksatsen om obligatoriskt användande av SGSI bli kostnadsdrivande i olika grad beroende på hur den regeln tillämpas.

**Sensorsystem, sidan 250**

Ekobrottsmyndigheten är kritisk till förslaget om obligatorisk användning av sensorsystem för identifiering av incidenter som rör it-säkerhet eftersom användningen av dessa sensorsystem och de rättsliga och integritetsmässiga konsekvenserna inte är närmare belysta eller analyserade.

Av betänkandet framgår att man med sensorsystem avser en kommunikationslösning med tekniska sensorer och en central funktion för analys av de avvikelser som uppmärksammas av sensorerna. Sensorerna skannar den trafik som går till och från t.ex. Ekobrottsmyndigheten och om någon information aktiverar sensorerna går ett larm till en central analysfunktion och eventuellt även till den verksamhet som blivit utsatt för ett ev. it-angrepp.

Vilka särskilda krav på sensorsystem som ska ställas på myndigheterna anges inte. Av 20 § i författningsförslaget framgår dock att Myndigheten för samhällsskydd och beredskap får

meddela de föreskrifter som behövs för verkställigheten av de allmänna och särskilda krav på statliga myndigheters informationssäkerhetsarbete som bl.a. avses i 11 §.

Användning av sensorssystem innebär, om de ska användas på kommunikation till och från Ekobrottsmyndigheten, behandling av personuppgifter. Användningen innebär också att, för det fall någon central funktion för analys utnyttjas, t.ex. FRA, att sekretessreglerad information kommer att hanteras utanför den verksamhet där informationen är skyddad av sekretess. I utredningens övervägande påtalas att vissa rättsfrågor inom områdena sekretess och personuppgiftsbehandling måste analyseras ytterligare. Någon egen analys har utredningen inte redovisat.

Enligt Ekobrottsmyndighetens uppfattning måste man ifrågasätta det lämpliga i att utredningen inte gjort någon egen analys av viktiga integritets- och sekretessfrågor som aktualiseras i det författningsförslag som man lägger fram. Vem förväntar sig utredningen ska göra dessa analyser när författningsförslaget öppnat för detaljreglering genom myndighetsföreskrift?

Ekobrottsmyndigheten ser det som rimligt att anta att en bred övervakning genom sensorsystem av den elektroniska trafiken till och från myndigheter kan skapa förtroendeskadliga situationer för både enskilda myndigheter och för e-förvaltningen. Särskilt som användningen av dessa sensorsystem och de rättsliga konsekvenserna inte är närmare belysta eller analyserade. Någon allmän diskussion kring övervakningen av elektronisk trafik mellan myndigheter och mellan myndigheter och enskilda har inte heller förts vilket i sig kan skapa frågor kring enskildas förtroende för myndigheternas hantering av information.

**Spårbar tid, sidan 251**
Ekobrottsmyndigheten stödjer förslaget om att nya tjänster för mer noggranna tidsangivelser införs. SP Sveriges Tekniska Forskningsinstitut har idag funktioner för kalibrering av tid med utökad noggrannhet och de redan existerande funktionerna bör användas för utbyggnaden.

### 9.4.2 Säkra kryptografiska funktioner, sidan 254
Ekobrottsmyndigheten stödjer de förslag som beskrivs i bilaga 4 för att ge MSB, FRA, FMV och FM uppdrag att utveckla processen för säkra kryptografiska funktioner för användning vid kommunikation internt inom statsförvaltningen.

Ekobrottsmyndigheten vill dock understryka att de statliga myndigheterna även har ett växande behov av att skydda kommunikation med utländska myndigheter samt med enskilda såväl i Sverige som i utlandet. Utredningen ger inget stöd när det gäller kompetens och samverkan vid val av produkter och lösningar i dessa sammanhang. Även om det inte är relevant att reglera sådan kryptering i förordning så bör en utpekad myndighet ha ett samordningsuppdrag här.

## Avsnitt 9.5 Incidentrapportering, sidan 257

Ekobrottsmyndigheten stödjer förslaget om informationssäkerhetsrelaterade lägesbeskrivningar, men ser även här ett behov av sekretessreglering för vissa uppgifter.

Ekobrottsmyndigheten ser behovet av en obligatorisk incidentrapportering för vissa allvarliga incidenter som rör informationssäkerhet. Trots att frågan utretts tidigare är det dock Ekobrottsmyndighetens bedömning att det fortfarande saknas vissa nödvändiga förutsättningar för ett införande via förordning.

Viktiga förutsättningar är förutom tekniska stödsystem och tillräckliga resurser även möjligheter att med sekretess skydda vissa tekniska uppgifter och personuppgifter som kan förekomma både i incidentrapporterna och i den respons som den rapporterande myndigheten behöver få tillgång till. Betänkandet innehåller inte tillräcklig information om vad som ska rapporteras utan anger allmänt att det avser *it-incidenter som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för.* Då betänkandet därutöver föreslår att MSB ska få ett öppet bemyndigande att föreskriva hur ett genomförande bör ske kan Ekobrottsmyndigheten inte bedöma konsekvenser av förslaget i dess nuvarande form.

Ekobrottsmyndigheten ser en utmaning då incidenter inträffar som berör informationssystem som omfattas av säkerhetsskydd och då särskilt när it-infrastruktur omfattas. Det är inte ovanligt att händelseförloppet för en incident är utsträckt och det är inte alltid känt initialt vilka tillgångar och system som är berörda. Av detta skäl riskerar osäkerhet eller felaktigheter uppstå då det ska beslutas till vilken myndighet incidenten ska rapporteras. Ekobrottsmyndigheten föreslår att särskild hänsyn tas till detta när förslaget bereds vidare.

## Avsnitt 9.6 Brottsbekämpning, sidan 262

Ekobrottsmyndigheten anser det vara angeläget att knyta an till det som i betänkandet sägs om brottsbekämpning och då i synnerhet om tvångsmedel i den digitala miljön.

### 9.6.1 It-brottskonventionen, sidan 262

Myndigheten instämmer i att Europarådets konvention om it-relaterad brottslighet bör ratificeras. På sikt bör fler myndighetsområden komma i fråga för sådant reglerat samarbete som krävs med den så snabbt ökande, internationella digitaliseringen.

### 9.6.2 Informationsutbyte, sidan 263

Ekobrottsmyndigheten är positivt till en översyn av om en tydligare reglering kan införas i offentlighets- och sekretesslagen rörande sekretess för uppgifter som utbyts vid samverkan mellan brottsbekämpande myndigheter och andra myndigheter inom informations- och cybersäkerhetsområdet.

Ekobrottsmyndigheten anser dock att denna översyn bör även omfatta behovet av sekretessreglering av informationsutbyte mellan andra myndigheter. Tydligare sekretessreglering kan behövas även för information i incidentrapporter, respons, lägesrapporter, sensorsystembehandling m.m.

### 9.6.3 Översyn av bestämmelser om tvångsmedel i den digitala miljön, sidan 264

Som konstateras i betänkandet sker elektronisk lagring av uppgifter i allt större utsträckning på annan plats än där personer eller verksamheter finns och det sker allt oftare på en server som finns i utlandet. Härtill kommer att bilden kompliceras ytterligare genom de snabbt ökande s.k. molntjänsterna, där uppgifterna kan vara lagrade var som helst i världen - på en eller flera platser. Många gånger är dessa uppgifter digitalt låsta, i den meningen att de inte är öppet tillgängliga för envar på internet.

Ekobrottsmyndigheten instämmer i att det behövs en genomgripande och detaljerad genomgång och analys och vill framhålla att det är viktigt att även andra tvångsmedel än de straffprocessuella inbegrips. En förnyad utredning om tillämpning av tvångsmedel i den digitala miljön skulle vara värdefull.

## Avsnitt 9.8 Övriga förslag, sidan 271

### 9.8.2 Fördjupad dialog om kompetensförsörjning, sidan 273

Utredaren nämner att Försvarshögskolans CIAO-utbildning skulle kunna vara ett kompetenskrav för informationssäkerhetschefer. Ekobrottsmyndigheten vill framhålla att utöver att alla statsanställda behöver en bred generell kompetensuppbyggnad så finns det flera personalkategorier som har behov av riktad kompetensuppbyggnad inom informationssäkerhet, exempelvis chefer eller personal inom IT och inköp.

## Avsnitt 10 Konsekvenser av förslagen, sidan 277

Som anges på sid 277 innebär utredningens förslag en höjd ambitionsnivå för statens informationssäkerhet men åtskilliga av åtgärdsförslagen kan ändå rymmas inom myndigheternas befintliga budget. Ekobrottsmyndigheten håller med om att MSB behöver en viss utökad budget, men anser i övrigt att utredaren underskattar behovet av ökad resursåtgång vid andra myndigheter.

Dessutom anser Ekobrottsmyndigheten det inte vara relevant eller korrekt (sid 282) att framhålla att kostnaderna kan antas vara marginella jämfört med de totala verksamhetskostnaderna. Så må vara fallet, men om den föreslagna strategin med alla åtgärder skulle genomföras på så kort tid som utredaren föreslår skulle det medföra behov av smärtsamma omprioriteringar i flertalet myndigheters verksamhetsplanering och budgetar.

Exempel på arbetsuppgifter som åtminstone för flera myndigheter kommer att medföra ökade kostnader och ökad resursåtgång är följande:

- Kravet i förordningen 7 § om att kartlägga sina informationsprocesser.
- Den nya nationella styrmodellen (oklart innehåll som på kort sikt bedöms kostnadsdrivande).
- Ökad resursåtgång för att bli en kvalificerad kravställare.
- Kravet på att använda certifierade och säkra produkter.
- Vidareutveckling, drift och förvaltning av de it-system som ska använda SGSI.
- Den nya obligatoriska incidentrapporteringen (oklart exakt hur).
- De nya obligatoriska sensorsystemen (oklart exakt hur).

---

Detta yttrande har beslutats av generaldirektören. I ärendets slutliga handläggning har chefsjuristen Lena Lindgren Schelin och verksarkivarie Sarah Mared deltagit. Verksamhetsskyddschef Carl Hedin har varit föredragande.

*Eva Fröjelin*

*Carl Hedin*

Kopia till

Justitiedepartementet/Å