Rättsenheten

Datum
2015-09-14

Diarienummer
2015-10768-2

Mottagare
Justitiedepartementet

Remissvar: Betänkandet SOU 2015:23 Informations- och cybersäkerhet Sverige - Strategi och åtgärder för säker information i staten

(Ju2015/2650/SSK)

Säkerhetspolisen har tagit del av betänkandet SOU 2015:23 Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten av utredningen som antagit namnet NISU 2014. Säkerhetspolisen har följande synpunkter.

Sammanfattning

Säkerhetspolisen välkomnar en bred ambitionshöjning på informationssäkerhetsområdet men förutsätter att författningsförslagen bereds och anpassas efter förslagen i betänkandet En ny säkerhetsskyddslag SOU 2015:25 som lämnats av utredningen om säkerhetsskyddslagen. Säkerhetspolisen vill därtill understryka vikten av samordning mellan säkerhetsskyddsåtgärden informationssäkerhet och informationssäkerhet i stort.

Säkerhetspolisen instämmer med direktivets utgångspunkter att informationssäkerheten i Sverige behöver stärkas, att det krävs en helhetssyn och att alla relevanta aktörer inkluderas. Det är dock tveksamt om den föreslagna strategin svarar mot denna behovsbeskrivning eftersom privata aktörer exkluderas och att förslaget till ny förordning inte avgränsar vilka uppgifter hos statliga myndigheter som behöver skyddas. När det gäller styrmodellen kan det visserligen vara ekonomiskt försvarbart att ta fram ett gemensamt ramverk men det är inte ekonomiskt försvarbart att alla verksamheter vidtar samma informationssäkerhetsåtgärder oavsett skyddsvärde. När det gäller förslaget att inrätta ett myndighetsråd bör det övervägas om ett sådant forum måste författningsregleras. En utvärdering av arbetet som görs inom det existerande forumet SAMFI (samverkansgruppen

Postadress
Box 12312
102 28 Stockholm

Besöksadress
Bolstomtavägen 2
171 69 Solna

Telefon
010-568 70 00
+46-10-568 70 00

Telefax
010-568 70 10
+46-10-568 70 10

E-post/Internet
sakerhetspolisen@sakerhetspolisen.se
www.sakerhetspolisen.se

för informationssäkerhet) bör göras. Säkerhetspolisen ställer sig vidare tveksam till utredningens utgångspunkter i föreslagen förordning. Förordningen är informationsorienterad men anger inte vilken typ av uppgifter som ska skyddas. Den gäller endast myndigheter trots utvecklingen att enskilda i högre grad är en del av samhällsviktig verksamhet. Författningsförslaget bör beredas efter förslagen som lämnats av utredningen om säkerhetsskyddslagen (SOU 2015:25). Säkerhetspolisen kan se vissa tillämpningsproblem med ytterligare en tillsynsmyndighet inom informationssäkerhetsområdet och samordning blir därför extra viktigt för att undvika överlappande ansvar. Säkerhetspolisen delar utredningens bedömning när det gäller myndigheters revision av informationssäkerhet. När det gäller regleringen om upphandling av it-system så tenderar placeringen i förordningen att leda till en svåröverskådlig upphandlingslagstiftning. Säkerhetspolisen har ingen erinran mot förslaget om obligatorisk it-incidentrapportering som sådant men bestämmelsen bör utformas utifrån förslaget om anmälan vid allvarlig säkerhetshotande verksamhet (10 kap. 2 § i förslag till säkerhetsskyddsförordning i SOU 2015:25). Säkerhetspolisen är tveksam till utredningens bedömning att åtgärdsförslagen i förordningen ryms inom myndigheternas befintliga budgetar med tanke på de sammantagna effekterna av föreslagna krav samt att förordningen utan urskiljning inkluderar all informationshantering.

1 Författningsförslag

1.1 Förslag till förordning för statliga myndigheters informationssäkerhet

Inledande bestämmelser

1 §

Vilken typ av information? Hur ska den skyddas? Aspekter på informationssäkerhet

Säkerhetspolisen är tveksam till utredningens utgångspunkter vid utformande av förslag till ny förordning. Utredningen har valt att göra förordningen informationsorienterad men regelverket utgår inte från en viss typ av information och beskriver inte hur den ska skyddas (jfr SOU 2015:25, s. 249). I stället omfattas all informationshantering hos statliga myndigheter vilket kommer medföra negativa konsekvenser för myndigheternas effektivitet och administration. Vidare fokuserar förordningen enbart på administrativ säkerhet och it-säkerhet. Även fysisk säkerhet och personalsäkerhet är viktiga aspekter i sammanhanget. IT-utvecklingen har medfört att säkerhetsskyddsåtgärder avseende informationssäkerhet och fysisk säkerhet alltmer har kommit att vävas samman. Ett exempel på det är att utökade möjligheter för medarbetare

Postadress Box 12312 102 28 Stockholm
Besöksadress Bolstomtavägen 2 171 69 Solna
Telefon 010-568 70 00 +46-10-568 70 00
Telefax 010-568 70 10 +46-10-568 70 10
E-post/Internet sakerhetspolisen@sakerhetspolisen.se www.sakerhetspolisen.se

att utföra sitt arbete från annat ställe än den fysiska arbetsplatsen medför ändrade förutsättningar för tillträdesskyddet.

Kommuner, landsting och enskilda exkluderade

Förordningen exkluderar kommuner, landsting och enskilda. Det kan ifrågasättas utifrån den inom säkerhetsskyddslagstiftningen rådande principen att skyddet av det skyddsvärda ska vara detsamma oavsett var uppgifterna förekommer (jfr prop. 1995/96:129, s. 35, Säkerhetsskydd). Även mot bakgrund av kommittédirektiven och behovet av samhällets informationssäkerhetsarbete i stort framstår det som mindre lämpligt att utelämna dessa aktörer. Samhällsviktig verksamhet bedrivs numera i stor utsträckning i privat regi, vilket utredningen också konstaterar i avsnitt 4.4.3 angående industriella informations- och styrsystem som till största delen hanteras av privata aktörer. Det bör därför övervägas att justera förordningen till att både omfatta allmän och enskild verksamhet. I den fortsatta beredningen bör även de erfarenheter som framkommit när det gäller brister i tillämpningen av säkerhetsskyddslagen tas tillvara.

All informationshantering eller endast elektronisk?

Mot bakgrund av vad som anges i kommittédirektiven borde det övervägas om förordningen endast avser elektronisk informationshantering.

2 §

Förordningen bör göras subsidiär

Förordningen bör göras subsidiär i förhållande till annan författning. Ett skäl till det är att undvika dubbelarbete hos myndigheter på informationssäkerhetsområdet, t.ex. när det gäller risk- och sårbarhetsanalyser eller liknande som krävs enligt annan lagstiftning om det har samma syfte som förordningen (jfr 3 § i Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet, MSBFS 2009:10, fn under översyn). Ett annat skäl kan vara att undvika att myndigheter får flera tillsynsmyndigheter inom informationssäkerhetsområdet.

Postadress Box 12312 102 28 Stockholm
Besöksadress Bolstomtavägen 2 171 69 Solna
Telefon 010-568 70 00 +46-10-568 70 00
Telefax 010-568 70 10 +46-10-568 70 10
E-post/Internet sakerhetspolisen@sakerhetspolisen.se www.sakerhetspolisen.se

Definitioner

4 §

Dubbelreglering av begreppet informationssäkerhet i lag och förordning

Säkerhetspolisen vill uppmärksamma att utredningen om säkerhetsskyddslagen valt att behålla begreppet informationssäkerhet (SOU 2015:25, s. 347). I utredningens förslag till säkerhetsskyddslag anges informationssäkerhet som en säkerhetsskyddsåtgärd som ska förebygga dels att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, dels skadlig inverkan på andra informationstillgångar som avser säkerhetskänslig verksamhet (2 kap. 1 § 1). I och med att NISU 2014 föreslår en ny definition om informationssäkerhet som en *förmåga att upprätthålla konfidentialitet, riktighet, tillgänglighet och spårbarhet i sin informationshantering* skapas en dubbelreglering av begreppet med olika betydelser. Om två definitioner av samma begrepp ska existera i olika författningar är det viktigt att det inte leder till tveksamheter för tillämpande myndigheter om vad som gäller på säkerhetsskyddsområdet. Eventuellt överlappande tillsynsområden måste också uppmärksammas och samordnas i författningsförslagen.

Myndighetens informationssäkerhetsarbete

8 §

Samordning av risk- och sårbarhetsanalyser i annan lagstiftning

Bestämmelsen bör kompletteras med en skrivning om att risk- och sårbarhetsanalyser får samordnas med andra liknande analyser som följer av annan författning. De flesta verksamheter i dag har krav på sig att genomföra olika typer av risk- och sårbarhetsanalyser. Säkerhetsskyddsanalys kan nämnas som exempel. Det är angeläget att i arbetet med risk- och sårbarhetsanalyser ta vara på den kunskap och de erfarenheter och de resultat som redan finns i organisationen på risk- och sårbarhetsområdet inte minst för att undvika dubbelarbete.

9 § andra stycket

Hur ska nivån på informationssäkerhet mätas och vad är en god förmåga?

Bestämmelsen ställer bl.a. krav på myndigheter att upprätthålla en viss nivå av informationssäkerhet men anger inte hur nivån ska mätas vilket kan leda till tillämpningsproblem. Vidare kan det vara svårt för myndigheter att avgöra vad en *god förmåga att hantera uppgifter* innebär. Innebörden av *sådan nivå* och *god förmåga* bör därför meddelas i verkställighetsföreskrifter enligt 20 §.

Postadress Box 12312 102 28 Stockholm
Besöksadress Bolstomtavägen 2 171 69 Solna
Telefon 010-568 70 00 +46-10-568 70 00
Telefax 010-568 70 10 +46-10-568 70 10
E-post/Internet sakerhetspolisen@sakerhetspolisen.se www.sakerhetspolisen.se

10 §

Definition av värdmyndighet

Det är tveksamt om begreppet *värdmyndighet* är vedertaget och det borde därför ha en egen definition i förordningen. Det är vidare oklart vilken myndighet som ska rapportera it-incidenter enligt 17 §, värdmyndigheten eller den anlitande myndigheten?

Särskilda krav på informationssäkerhetsarbete

11 §

Det bör bl.a. säkerställas att kraven i den föreslagna bestämmelsen i 11 § inte går utöver den föreslagna säkerhetsskyddslagstiftningens krav. Bestämmelsen, som ställer särskilda krav på informationssäkerhetsarbete för de s.k. krisberedskapsansvariga myndigheterna i 11 § förordningen (2006:942) om krisberedskap och höjd beredskap, bör i det fortsatta lagstiftningsarbetet stämmas av mot 2 kap. 2 § i förslag till säkerhetsskyddslag som innehåller skyldigheter för den som är ansvarig för en säkerhetskänslig verksamhet. Vidare bör bestämmelsen stämmas av mot 4 kap. 3 § i förslag till säkerhetsskyddsförordning som innehåller vilka funktioner som ett it-system som ska användas av flera personer för behandling av säkerhetsskyddsklassificerade uppgifter ska innehålla (SOU 2015:25, s. 55 och 86).

Upphandling och utveckling av it-system och it-produkter

15-16 §§

Bestämmelsernas placering

Aktuella bestämmelser som rör kravställning av informationssäkerhetsaspekter vid upphandling borde vara lämpligare att placera i gällande upphandlingslagstiftning. Aktuell placering kan i förlängningen göra upphandlingslagstiftningen svåröverskådlig.

Behov av definition av it-system

Säkerhetspolisen anser att begreppet *it-system* borde ha en definition i förordningen (jfr 1 kap. 7 § i förslag till säkerhetsskyddsförordning, SOU 2015:25, s. 82). Avsaknaden av en definition är en brist mot bakgrund av vad utredningen återger på s. 162 i betänkandet: *Industriella informations- och styrsystem "faller mellan stolarna" och betraktas inte som it-system utan som produktionssystem. Det*

kan få till följd att det inte finns någon som tar ansvar för säkerheten i dessa system eller ställer krav på att säkerheten ska utvecklas.

Samordning av informationsklassificering

Det bör framgå att informationsklassificering i 15 § andra stycket (av utredningen benämnt informationsklassning) får samordnas med den informationsklassificering som ska ske enligt den föreslagna säkerhetsskyddslagstiftningen (SOU 2015:25, s. 331 ff.).

Olika formuleringar beskriver samma sak?

Det bör påpekas att 15 § fjärde stycket sista meningen som innehåller formuleringen *kan ha påverkat säkerheten* skiljer sig från formuleringen i 17 § första stycket som lyder *som allvarligt kan påverka säkerheten*. Det är oklart om denna nyansskillnad är avsedd och vad den i så fall syftar till.

16 §

Utpekande av produkter i verkställighetsföreskrifter förenligt med upphandlingslagstiftningen?

Bestämmelsen som ålägger myndigheter att använda säkra it-produkter som är tänkt att utpekas i verkställighetsföreskrifter är en god ambition men bör utredas i förhållande till upphandlingslagstiftningen, t.ex. de grundläggande principerna om likabehandling och proportionalitet. Att staten rekommenderar vissa produkter blir en konkurrensfördel för vissa leverantörer och frågan är om det är förenligt med den s.k. likabehandlingsprincipen. Vidare kan alltför långtgående krav som inte har en tydlig och affärsmässig koppling till kontraktsföremålet strida mot den s.k. proportionalitetsprincipen. Kravet på proportionalitet kan bl.a. innebära att en upphandlande myndighet måste acceptera likvärdiga kvalitetssäkringsåtgärder. Det är då inte säkert att regleringen får avsedd effekt.

It-incidentrapportering

17 §

Obligatorisk it-incidentrapportering

Säkerhetspolisen har ingen erinran mot förslaget till obligatorisk it-incidentrapportering som sådant. Det bör dock övervägas om formuleringen *allvarligt kan påverka säkerheten* är ändamålsenlig eller om den bör ersättas med uttrycket *allvarligt kan skada verksamheten* för att bättre avgränsa i vilka situationer myndigheter ska rapportera it-incidenter. Säkerhetspolisen anser att det förslag som lagts av utredningen av säkerhetsskyddslagen i 10 kap. 2 § i förslag till

Postadress Box 12312 102 28 Stockholm
Besöksadress Bolstomtavägen 2 171 69 Solna
Telefon 010-568 70 00 +46-10-568 70 00
Telefax 010-568 70 10 +46-10-568 70 10
E-post/Internet sakerhetspolisen@sakerhetspolisen.se www.sakerhetspolisen.se

säkerhetsskyddsförordning bör tjäna som utgångspunkt i den fortsatta beredningen (SOU 2015:25, s. 95). Förslagsvis ska en myndighet, förutom när det gäller röjande av hemliga uppgifter, skyndsamt anmäla till aktuell tillsynsmyndighet enligt nuvarande 39 § säkerhetsskyddsförordningen även i annat fall om det inträffat en it-incident som kan orsaka allvarlig skada för rikets säkerhet (nuvarande uttryck). Om en sådan anmälan har rapporterats till Försvarsmakten, ska Försvarsmakten skyndsamt informera Säkerhetspolisen om it-incidenten. Skälet till det är att Säkerhetspolisen behöver överväga om en förundersökning ska inledas men även för att kunna sammanställa en lägesbild över sådana incidenter.

Tillsyn, föreskrifter och myndighetsrådets uppgifter

19 §

Om ytterligare en myndighet ska utöva tillsyn inom området för informationssäkerhet bör författningstexten bättre uttrycka hur arbetet ska samordnas med befintliga tillsynsmyndigheterna inom säkerhetsskyddsområdet för att undvika överlappande tillsynsansvar. Detta kommer inte till uttryck i förordningens 19 §. Det bör alltså utredas om det blir fråga om dubbelreglering och hur eventuell dubbel tillsynsverksamhet mellan Säkerhetspolisen, Försvarsmakten och Myndigheten för samhällsskydd och beredskap ska organiseras på ett effektivt och ändamålsenligt sätt. Lämpligheten i att myndigheter kan få flera tillsynsmyndigheter i fråga om informationssäkerhet bör utredas. I detta sammanhang vill Säkerhetspolisen lyfta fram den uppfattning som utredningen av säkerhetsskyddslagen återger i sitt betänkande (SOU 2015:25, s. 347):

Åtgärder som är förknippade med informationssäkerheten enligt säkerhetsskyddslagen kan inte särskiljas från informationssäkerhet i en vidare bemärkelse. Exempel på detta är skydd mot skadlig kod och användarautentisering som är relevanta åtgärder även för it-system som inte är av betydelse för Sveriges säkerhet. Föreskrifter som meddelas med stöd av lagstiftningen, måste kunna avse informationssäkerheten i stort för de verksamheter som omfattas av säkerhetsskyddslagens krav. Detsamma gäller för tillsyn. En helhetssyn krävs inom detta område och såväl föreskrifter som tillsyn måste kunna omfatta samtliga de relevanta åtgärder som syftar till att ge ett skydd för information.

Säkerhetspolisen delar utredningens uppfattning som återges ovan.

20 §

Säkerhetspolisen instämmer med utredningen att det bör utredas om det finns ett behov av samordning avseende till vilken myndighet som återrapportering ska ske när det gäller it-produkter som omfattas av säkerhetsskyddslagens krav (se s. 240).

1.2 Förslag till förordning om ändring i säkerhetsskyddsförordning (1996:633)

10 a §

Säkerhetspolisen förordar att förslaget om anmälan vid allvarlig säkerhetshotande verksamhet i 10 kap. 2 § i förslag till säkerhetsskyddsförordning i betänkandet SOU 2015:25 införs (s. 95) ska tjäna som utgångspunkt i den fortsatta beredningen av obligatorisk it-incidentrapportering.

2 Uppdragets genomförande och begrepp

2.3 Utredningens inriktning

Säkerhetspolisen anser att utredningens inriktning vilar på en tveksam utgångspunkt nämligen att det enkelt går att åtskilja säkerhetsskyddsåtgärden informationssäkerhet och informationssäkerhet i vidare bemärkelse utan samordning. Det går inte att komma ifrån att säkerhetsskyddsåtgärden informationssäkerhet har en samverkande effekt på informationssäkerhet i det större perspektivet. Säkerhetspolisen vill i sammanhanget citera betänkandet av utredningen om säkerhetsskyddslagen som skriver bl.a. (SOU 2015:25, s. 240):

När det gäller informationssäkerhet bedrivs i dag ett arbete på bred front med att stärka samhällets informationssäkerhet. Detta innebär att ett stort antal myndigheter m.fl. arbetar med informationssäkerhetsfrågor, dock utifrån andra utgångspunkter än att betrakta informationssäkerheten som en säkerhetsskyddsangelägenhet. Att informationssäkerhetsarbetet bedrivs utifrån diverse utgångspunkter med stöd av olika författningar kan ge upphov till tveksamheter för tillämpande myndigheter och övriga om vad det är som särskilt gäller för informationssäkerhet på säkerhetsskyddsområdet.

Säkerhetspolisen delar utredningen om säkerhetsskyddslagens beskrivning ovan.

Sedan säkerhetsskyddslagens (1996:627) tillkomst har behovet av säkerhetsskydd och andra former av skydd utsträckts till att omfatta fler verksamheter än tidigare. Även verksamheter och funktioner som inte täcks av säkerhetsskyddslagen kan ha skyddsbehov. Detta får tillgodoses genom annan reglering. Det finns sådan reglering i dag som kan utvecklas. Exempelvis förordningen (2006:942) om krisberedskap och höjd beredskap. Vidare träffas myndigheters information av de föreskrifter om statliga myndigheters informationssäkerhet som Myndigheten för samhällsskydd och beredskap har meddelat (MSBFS 2009:10 med stöd av 34 § förordningen (2006:942) om krisberedskap och höjd beredskap som fn är föremål för översyn). Verksamheter och funktioner som inte omfattas av säkerhetsskyddslagen kan ändå med fördel samordnas med säkerhetsskyddsåtgärder, inte minst av kostnads- och effektivitetsskäl. Säkerhetspolisen anser att detta inte kommer fram i utredningens förslag i tillräcklig grad. Tvärtom kan förslagen ytterligare bidra till tveksamheter för tillämpande myndigheter. Om förslag till förordning för statliga myndigheters informationssäkerhet leder till lagstiftning, måste det ske utifrån den utgångspunkt som illustrerats ovan, nämligen att säkerhetsskyddsåtgärden informationssäkerhet samordnas med informationssäkerhet i det större perspektivet.

9 Överväganden och förslag

9.1 En nationell strategi för statens informations- och cybersäkerhet

9.1.3 Behovet av en strategi

Utredningens direktiv var att föreslå övergripande mål för samhällets informationssäkerhetsarbete. I dag hanterar kommuner, landsting och privata näringsidkare i princip samma typ av uppgifter som myndigheter hanterar. Inom säkerhetsskyddet finns en viktig princip som även gör sig gällande för informationssäkerhet i vidare bemärkelse. Skyddet av information ska vara detsamma oavsett vem som hanterar uppgiften. Således räcker det inte med att endast ställa krav på statliga myndigheter. Informationssäkerhet kräver en helhetssyn och även det privata näringslivet måste inkluderas.

Vidare borde en bättre utgångspunkt för utredningen ha varit att analysera *vad* som ska skyddas i stället för att som nu inkludera all informationshantering. Säkerhetspolisen anser att en lämpligare utgångspunkt för strategin skulle vara att reglera informationssäkerheten för sekretessbelagda uppgifter samt uppgifter hos enskilda som varit sekretessbelagda om de hade hanterats hos en myndighet. Ett sådant angreppssätt skulle underlätta avgränsningen av skyddsvärda uppgifter i samhället även om de inte når upp till nivån rikets (Sveriges) säkerhet. En sådan utgångspunkt skulle också väl stämma överens med regeringens ökade fokus på det civila försvaret.

Postadress Box 12312 102 28 Stockholm
Besöksadress Bolstomtavägen 2 171 69 Solna
Telefon 010-568 70 00 +46-10-568 70 00
Telefax 010-568 70 10 +46-10-568 70 10
E-post/Internet sakerhetspolisen@sakerhetspolisen.se www.sakerhetspolisen.se

9.2 Ansvar, styrning, samordning och tillsyn

Säkerhetspolisen är tveksam till att inrätta en styrmodell, utöver nuvarande bestämmelser i förordningen (2006:942) om krisberedskap och höjd beredskap och Myndigheten för samhällsskydd och beredskaps föreskrifter, som syftar till att alla myndigheter i Sverige ska utföra sitt informationssäkerhetsarbete på samma sätt oavsett verksamhetens karaktär med avseende på skyddsvärde. Det kan vara ekonomiskt försvarbart att ta fram ett gemensamt ramverk men det är inte ekonomiskt försvarbart att alla verksamheter vidtar samma informationssäkerhetsåtgärder oavsett skyddsvärde. Åtgärder bör anpassas till myndigheternas verksamhet och inte tvärtom.

9.2.2 Inrättande av ett myndighetsråd

När det gäller förslaget att inrätta ett myndighetsråd bör det övervägas om ett sådant forum måste författningsregleras. En utvärdering av arbetet som görs inom det existerande forumet SAMFI (samverkansgruppen för informationssäkerhet) bör under alla omständigheter göras innan ett nytt forum övervägs. Säkerhetspolisen är vidare tveksam till att myndigheter ska ha en samrådsskyldighet med ett myndighetsråd innan de fattar beslut i sitt eget informationssäkerhetsarbete liksom att myndigheter ska överlämna uppgiften som remiss- och beredningsinstans till myndighetsrådet. Vidare anser Säkerhetspolisen inte att det är en lämplig uppgift för ett myndighetsråd att ge stöd till myndigheter. När det gäller sådant stöd inom upphandlingsområdet krävs expertkompetens inom det området om det överhuvudtaget ska göras. Det är dessutom en stor och resurskrävande uppgift vilket utredningen inte lyfter fram.

När det gäller verksamhet som bedrivits i SAMFI och övningsverksamhet bör en utvärdering av dessa verksamheter göras bland de som deltagit i verksamheterna innan nya förslag läggs som t.ex. ett nytt statligt myndighetsråd för informationssäkerhet.

9.2.5 Informationssäkerhet som en del av myndighets revision

Säkerhetspolisen delar utredningens bedömning.

10 Konsekvenser av förslagen

Konsekvenser av två regleringar beträffande myndigheters informationssäkerhetsarbete

Om föreslagen förordning för statliga myndigheters informationssäkerhet ska förekomma parallellt med den nya säkerhetsskyddslagen (se SOU 2015:25) bör den nya förordningen göras sekundär och begreppsbildningen i den bör analyseras och samordnas mer. Vidare vore det önskvärt om det av förordningstexten framgår att myndigheters informationssäkerhetsarbete får samordnas med det arbete som myndigheter redan är skyldiga att utföra enligt säkerhetsskyddslagen, t.ex. att upprätta en säkerhetsskyddsanalys. Allt i syfte att undvika dubbelt informationssäkerhetsarbete. Risk- och sårbarhetsanalyser och säkerhetsskyddsanalyser har mycket gemensamt. Utredningen av säkerhetsskyddslagen föreslår att utvidga den nya säkerhetsskyddslagens tillämpningsområde till att ge skydd även för s.k. säkerhetskänslig verksamhet, t.ex. styrning och hantering av samhällskritiska it-system, el- och energiförsörjning, sammanställningar av uppgifter som är av central betydelse för ett fungerande samhälle eller verksamhet som behöver skyddas på den grunden att den omfattar sådant som kan skada nationen. Förslagen från NISU 2014 överlappar i allt väsentligt med en ny utvidgad säkerhetsskyddslag. I den mån förslagen inte är förenliga måste det hanteras i den fortsatta beredningen.

Det förhållandet att vissa myndigheter kommer att få flera tillsynsmyndigheter på informationssäkerhetsområdet bör också uppmärksammas och analyseras i det fortsatta lagstiftningsarbetet.

Kostnadskonsekvenser

All informationshantering hos statliga myndigheter omfattas av förslaget. Därför kommer förslaget leda till en betydande kostnadsökning och minskad effektivitet hos statliga myndigheter. Informationssäkerheten bör kunna dimensioneras utifrån uppgifternas skyddsvärde vilket dock inte kommer till uttryck i den föreslagna förordningen. En grundligare analys om vilken information som är skyddsvärd i samhället sett utifrån förordningens syfte borde därför ha gjorts. Erfarenheter från säkerhetsskyddsområdet visar att det redan för mycket skyddsvärda uppgifter, sådana som rör Sveriges säkerhet, är svårt att få till stånd ett väl anpassat skydd, just mot bakgrund av kostnader och hinder mot en effektiv verksamhet. Det är en av anledningarna till att säkerhetsskyddslagen är under översyn. Säkerhetspolisen saknar en diskussion om att ökade krav på informationssäkerhetsåtgärder medför ökade kostnader och en mindre effektiv verksamhet men att regleringen ändå är motiverad.

Postadress Box 12312 102 28 Stockholm
Besöksadress Bolstomtavägen 2 171 69 Solna
Telefon 010-568 70 00 +46-10-568 70 00
Telefax 010-568 70 10 +46-10-568 70 10
E-post/Internet sakerhetspolisen@sakerhetspolisen.se www.sakerhetspolisen.se

Säkerhetspolischefen Anders Thornberg har beslutat detta yttrande.

Postadress Box 12312 102 28 Stockholm
Besöksadress Bolstomtavägen 2 171 69 Solna
Telefon 010-568 70 00 +46-10-568 70 00
Telefax 010-568 70 10 +46-10-568 70 10
E-post/Internet sakerhetspolisen@sakerhetspolisen.se www.sakerhetspolisen.se