Kommittédirektiv

Genomförande av EU-direktiv om åtgärder för en hög gemensam nivå av säkerhet i nätverk och informationssystem

Dir. 2016:29

Beslut vid regeringssammanträde den 31 mars 2016

Sammanfattning

En särskild utredare ska föreslå hur EU-direktivet om åtgärder för en hög gemensam nivå av säkerhet i nätverk och informationssystem ska genomföras i svensk rätt.

Utredaren ska bl.a.

- föreslå hur direktivets krav på utpekande av myndigheter med ansvar för vissa funktioner ska genomföras, med inriktningen att Myndigheten för samhällsskydd och beredskap (MSB) ges en samordnande roll på området men att andra myndigheters ansvar för tillsyn inom särskilda sektorer ska fortsätta att gälla,
- föreslå hur identifiering av och krav på aktörer som omfattas av direktivet kan genomföras i ett samlat regelverk med beaktande av gällande bestämmelser, sektorsansvar och vad som är mest effektivt utifrån olika perspektiv,
- föreslå nödvändiga ändringar i offentlighets- och sekretesslagen (2009:400) för att känslig information i incidentrapporter ska kunna skyddas, och
- lämna nödvändiga författningsförslag.

Uppdraget ska redovisas senast den 1 maj 2017.

EU-direktivet och motsvarande svenska regler

Direktivet innehåller bl.a. skyldigheter för varje medlemsstat att anta en nationell strategi för säkerhet i nätverk och informationssystem och att utse myndigheter med särskilda uppgifter på detta område. Medlemsstaterna blir vidare skyldiga att identifiera operatörer som bedriver samhällsviktig verksamhet inom sju sektorer och som är beroende av nätverk och informationssystem. Sektorerna omfattar energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten och digital infrastruktur. Den aktuella sektorsindelningen innebär att kommunala verksamheter kan omfattas. För sådana aktörer innebär direktivet bl.a. att verksamheten kan komma att behöva anpassas för att uppnå en hög nivå av säkerhet i nätverk och informationssystem och att it-incidenter av viss dignitet ska rapporteras till behörig myndighet. Direktivet bedöms träda i kraft under våren 2016. Medlemsstaterna är skyldiga att ha genomfört direktivet senast 21 månader därefter.

Frågor som berör informations- och cybersäkerhet och särskilt hur it-incidenter ska förebyggas och hanteras har tidigare varit aktuella i ett flertal utredningar. Riksrevisionen har i en rapport från november 2014 (RiR 2014:23) funnit brister i regeringens arbete med informationssäkerhetsfrågor inom den civila statsförvaltningen. Granskningen föranledde Riksrevisionen att lämna ett flertal rekommendationer till regeringen och dess myndigheter. Riksrevisionen påpekade särskilt att det finns ett behov av att utreda hur tillsynen över informationssäkerheten kan samlas och koordineras på ett bättre sätt än i dag. Även i betänkandena Informations- och cybersäkerhet i Sverige (SOU 2015:23) och En ny säkerhetsskyddslag (SOU 2015:25) lämnas förslag på åtgärder inom informationssäkerhetsområdet.

Regeringen har konstaterat att delar av arbetet med informationssäkerhet i den civila statsförvaltningen inte har genomförts ändamålsenligt (skr. 2014/15:84). Som ett första steg för att förbättra samhällets förmåga att identifiera, begränsa och förhindra it-angrepp mot informationssystem i samhället,

har regeringen tagit initiativ till ett system för obligatorisk it-incidentrapportering för statliga myndigheter. De bestämmelser som införts i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap och i säkerhetsskyddsförordningen (1996:633) innebär att alla statliga myndigheter från den 1 april 2016 ska rapportera allvarliga it-incidenter till MSB eller, i vissa fall, till Säkerhetspolisen eller Försvarsmakten. Detta system utelämnar dock enskilda aktörer samt kommuner och landsting. Bestämmelser som rör it-incidentrapportering för enskilda aktörer finns i dag i begränsad utsträckning, t.ex. för de aktörer som omfattas av lagen (2003:389) om elektronisk kommunikation. Genomförandet av direktivet, som även omfattar andra aktörer än statliga myndigheter, i svensk rätt är därför av stor betydelse för att uppnå en förbättrad informations- och cybersäkerhet i samhället.

Uppdraget att föreslå hur EU-direktivet ska genomföras

Det är viktigt att säkerställa en hög nivå av säkerhet för nätverk och informationssystem inom ett antal sektorer i Sverige i enlighet med EU-direktivet. Hänsyn ska också tas till behovet av att skydda Sveriges säkerhet, behovet av en fungerande brottsbekämpning och myndigheters och företags behov av att kunna skydda känsliga uppgifter. Regelverket ska dock inte skapa en större administrativ börda för de enskilda aktörerna än nödvändigt för direktivets efterlevnad. Enkelhet, överskådlighet, konsekvens och kostnadseffektivitet ska eftersträvas.

Direktivet innebär ett antal långtgående skyldigheter för medlemsstaterna i och med de krav som direktivet ställer på att varje medlemsstat ska ta fram en nationell strategi, peka ut myndigheter med särskilt ansvar enligt direktivet och identifiera och ställa krav på de aktörer som berörs av bestämmelserna.

I betänkandet Informations- och cybersäkerhet i Sverige (SOU 2015:23) föreslås att regeringen ska anta en nationell strategi för statens informations- och cybersäkerhet. Betänkandet har remitterats och bereds för närvarande inom Regeringskansliet. Regeringen avser att prioritera detta arbete

och bedömer att strategin bör kunna anpassas för att motsvara direktivets krav på vad en nationell strategi för säkerhet i nätverk och informationssystemska innehålla. Frågan om hur en sådan strategi bör utformas omfattas således inte av utredarens uppdrag.

Hur ska ansvarsfördelningen mellan myndigheter i Sverige se ut?

Direktivet ålägger medlemsstaterna att utse en eller flera behöriga myndigheter som utövar tillsyn över direktivets genomförande och tillämpning. En viktig åtgärd för att direktivet ska kunna tillämpas är att medlemsstaternas tillsynsmyndigheter ges tillräckliga befogenheter för att kontrollera att aktörerna, d.v.s. operatörer som bedriver samhällsviktig verksamhet och leverantörer av digitala tjänster, följer direktivet. Myndigheterna ska därför enligt direktivet ha möjlighet att begära dels att aktörerna lämnar nödvändig information om säkerheten i sina nätverk och informationssystem, dels att de genomgår säkerhetsrevision. Medlemsstaterna ska också se till att tillsynsmyndigheten har tillgång till effektiva och proportionerliga sanktioner. I medlemsstaterna ska det även finnas ett eller flera incidenthanteringsorgan (s.k. CSIRT, Computer Security Incident Response Team) och en nationell kontaktpunkt för samarbetet med andra medlemsstater. Den nationella kontaktpunkten ska vara ansvarig för att samordna frågor om säkerhet i nätverk och informationssystem enligt direktivet och fungera som kontaktpunkt i gränsöverskridande frågor på unionsnivå.

Direktivet ställer också krav på ett formaliserat samarbete mellan medlemsstaterna, bl.a. när en medlemsstat identifierar operatörer som bedriver samhällsviktig verksamhet även i annan medlemsstat. Genom direktivet inrättas också en samarbetsgrupp där representanter för medlemsstaterna ska delta och ett formellt samarbete mellan de nationella organisationerna för CSIRT. Samarbetsgruppen är tänkt att ha en strategisk funktion medan medlemsstaterna inom ramen för ett särskilt CSIRT-nätverk bl.a. ska kunna utbyta operativ information och

diskutera specifika problem med koppling till inträffade it-incidenter.

MSB har i dag ett särskilt uppdrag inom samhällets informationssäkerhet. Enligt MSB:s instruktion ansvarar myndigheten bl.a. för att stödja och samordna arbetet med samhällets informationssäkerhet, i vilket ingår förebyggande arbete liksom även samordning och hantering vid inträffade it-incidenter. MSB svarar vidare för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter. Arbetet sker genom MSB:s CERT-verksamhet (Computer Emergency Response Team) och innebär därutöver att myndigheten är Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder, däribland CERT-EU. MSB har sedan funktionen fördes över till myndigheten från Post- och telestyrelsen fortsatt att bygga upp såväl kompetens som ett brett kontaktnät inom informations-säkerhetsområdet. Det finns flera myndigheter som utövar tillsyn över informationssäkerheten inom sina sektorer och som inom dessa områden är bemyndigade att utfärda föreskrifter. Detta gäller exempelvis Post- och telestyrelsen, Svenska kraftnät och Finansinspektionen. Även Säkerhetspolisen och Försvarsmakten utfärdar föreskrifter om bl.a. informations-säkerhet för verksamheter som omfattas av kraven i säkerhets-skyddslagen (1996:627). Den tillsyn som Säkerhetspolisen och Försvarsmakten genomför mot bakgrund av dessa föreskrifter faller utanför EU-direktivet eftersom det gäller nationell säkerhet. Detsamma gäller för elektroniska kommu-nikationstjänster, e-legitimationer och betrodda tjänster i enlighet med EU-direktivets artikel 1 (3).

Mot bakgrund av det uppdrag som MSB i dag har på informationssäkerhetsområdet och den kompetens som finns inom myndigheten bör Sveriges CSIRT-organisation finnas hos MSB och MSB anförtros rollen som nationell kontaktpunkt. Det innebär att det är till MSB som aktörerna ska rapportera it-incidenter i enlighet med EU-direktivets krav. Detta hindrar dock inte att aktörerna kan ha skyldighet att rapportera it-incidenter till den myndighet som har tillsynsansvar inom den

aktuella sektorn. I MSB:s roll bör det också ingå att delta i CSIRT-nätverket och i den samarbetsgrupp som skapas.

Tillsynsmyndigheterna inom de sektorer som omfattas av direktivet bör även fortsättningsvis ha kvar ansvaret för att kontrollera att aktörerna följer respektive sektors regler om informationssäkerhet. Det behöver analyseras om dessa myndigheters mandat behöver förändras för att uppfylla direktivets krav. För sådana aktörer som träffas av direktivet och där tillsyn över säkerheten i nätverk och informationssystem i dag saknas, behöver det övervägas vilken myndighet som kan anförtros uppgiften att utöva tillsyn. I avsaknad av andra myndigheter med tillsynsuppgifter inom den aktuella sektorn och inom informationssäkerhet, bör det utredas om MSB ska vara tillsynsmyndighet eller om uppgiften ska anförtros en myndighet med närliggande tillsynsuppgifter. Detta kan t.ex. övervägas inom olje- och gassektorn. Inriktningen bör vara att Post- och telestyrelsen ges fortsatt och vid behov kompletterande ansvar för tillsyn av de digitala infrastrukturer som nämns i EU-direktivets bilaga 2.

Då MSB redan i dag har ansvar för att samordna arbetet med samhällets informationssäkerhet bör MSB få en samordnande roll mellan tillsynsmyndigheterna. Utöver att vara CSIRT, nationell kontaktpunkt och att delta i samarbetsgrupperna innebär denna roll att MSB behöver få del av tillsynsrapporter från andra sektorsmyndigheter i syfte att få en samlad bild över EU-direktivets genomförande och tillämpning i Sverige. Detta medför dock inte något övertagande av sektorsmyndigheternas ansvar för tillsyn över aktörer eller något mandat att styra hur dessa myndigheter ska använda sina resurser.

Eftersom direktivet möjliggör för medlemsstaterna att skydda information som gäller nationell säkerhet är det av vikt att MSB och andra tillsynsmyndigheter, om de får del av information som omfattas av säkerhetsskyddslagstiftningen, samverkar med Säkerhetspolisen eller Försvarsmakten.

Utredaren ska

- föreslå hur MSB:s roll som CSIRT-organisation, nationell kontaktpunkt och deltagare i de samarbets-

nätverk som direktivet lägger grund för ska utformas och regleras, och

- lämna förslag på ett system för tillsyn i enlighet med direktivets krav, där befintliga myndigheter behåller eller kompletterar sina nuvarande roller, men där MSB ges en samordnande funktion.

Hur ska operatörer identifieras och vilka krav ska ställas på dem och leverantörer av digitala tjänster?

Direktivet ålägger medlemstaterna att identifiera de offentliga och enskilda operatörer som tillhandahåller samhällsviktiga tjänster inom ett antal särskilt utpekade sektorer och som är beroende av nätverk och informationssystem. Medlemsstaterna ska enligt direktivet införa regler som innebär att dessa aktörer ska vidta tekniska och organisatoriska åtgärder för att hantera säkerhetsrisker i sina nätverk och informationssystem och att rapportera allvarliga it-incidenter.

Vid sidan av operatörer som bedriver samhällsviktig verksamhet reglerar direktivet även på liknande sätt säkerheten i nätverk och informationssystem hos leverantörer av digitala tjänster, s.k. Digital Service Providers (DSP). I den kategorin ingår e-handelsplatser, sökmotorer och molntjänster. Gemensamt för dessa aktörer är att de tillhandahåller digitala tjänster över nationsgränserna och att en incident hos en sådan aktör skulle kunna medföra allvarlig påverkan på flera medlemsstaters samhällsviktiga verksamheter. Enligt direktivet ska alla leverantörer av digitala tjänster hanteras på samma sätt inom hela EU utifrån vad som är proportionerligt i förhållande till den risk som verksamheten kan utgöra. Medlemsstaterna är inte skyldiga att identifiera leverantörer av digitala tjänster men däremot att se till att även dessa aktörer vidtar tekniska och organisatoriska åtgärder för att hantera säkerhetsrisker mot nätverk och informationssystem och att de rapporterar allvarliga it-incidenter till tillsynsmyndigheten. Skyldigheten gäller enbart för den medlemsstat där en sådan aktör har sitt fasta etableringsställe eller en representant.

Det behöver mot denna bakgrund analyseras hur direktivets krav på identifiering av operatörer som bedriver samhällsviktig verksamhet och krav på aktörerna ska genomföras i svensk rätt. Analysen bör göras med utgångspunkten att det är verksamhetsutövaren som är ansvarig för att avgöra om denne omfattas av regelverket, vilket motsvarar vad som gäller enligt t.ex. säkerhetsskyddslagen (1996:627). I dag finns ett flertal regelverk som ställer krav på informationssäkerhet utifrån olika förutsättningar. I linje med regeringens ambition att verka för ett mer ändamålsenligt arbete med informationssäkerhet inom statsförvaltningen bör det utredas ifall direktivet, särskilt direktivets krav på operatörer som bedriver samhällsviktig verksamhet och leverantörer av digitala tjänster, bör genomföras i ett samlat regelverk om säkerhet för nätverk och informationssystem.

Direktivet tillåter medlemsstaterna att skydda information som gäller nationell säkerhet och information som kan påverka möjligheten att upprätthålla lag och ordning särskilt i fråga om brottsbekämpning. Det svenska systemet för obligatorisk it-incidentrapportering för statliga myndigheter har utformats på sådant sätt att it-incidenter i vissa särskilt säkerhetskänsliga system, inklusive incidenter som upptäckts genom stöd enligt 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt, i stället för till MSB ska rapporteras enligt säkerhetsskyddsförordningen till Säkerhetspolisen eller Försvarsmakten. Myndigheterna på försvarsområdet och försvarsindustrin omfattas inte av direktivets krav och dessa aktörers rapportering av it-incidenter ska med hänsyn till rikets säkerhet inte omfattas av den nya ordning som föreslås. Även it-incidenter hos andra aktörer som har upptäckts genom stöd enligt 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt (FRA) bör kunna undantas från direktivets tillämpning om rapporteringen innebär risk för att sekretesskyddade uppgifter om FRA:s förmåga röjs. Det kan även finnas andra aktörer som visserligen omfattas av direktivets krav men som ändå bör undantas från reglerna för att skydda information som gäller nationell säkerhet. It-incidenter som skulle röja information som gäller nationell säkerhet kan

dock även fortsättningsvis rapporteras enligt den ordning som från den 1 april 2016 gäller enligt säkerhetsskyddsförordningen.

Bestämmelser om informationssäkerhet i sektorsspecifika EU-rättsakter, som innehåller motsvarande eller mer långtgående krav, ska ha företräde framför de aktuella bestämmelserna i direktivet. Även detta bör beaktas i de överväganden som görs.

Enligt direktivet ska tillsynsmyndigheterna ha tillräckliga verktyg för att se till att regelverket efterlevs. I detta ligger ett sanktionssystem med effektiva och proportionerliga åtgärder. För svenskt vidkommande bör ett sådant system vara uppbyggt enligt den struktur som redan gäller i dag, d.v.s. att en tillsynsmyndighets beslut om sanktioner kan överklagas till allmän förvaltningsdomstol. Direktivet gör ingen åtskillnad mellan offentliga och enskilda aktörer. Frågan bör därför analyseras med utgångspunkt i att även offentliga aktörer, på lämpligt sätt, ska kunna åläggas sanktioner.

Utredaren ska, med beaktande av att direktivet inte hindrar medlemsstaterna från att skydda sina nationella säkerhetsintressen och de begränsningar som nämnts ovan,

- föreslå hur operatörer som bedriver samhällsviktig verksamhet i Sverige ska identifieras,
- föreslå hur direktivets krav på både operatörer som bedriver samhällsviktig verksamhet och leverantörer av digitala tjänster bör genomföras i svensk rätt, och
- analysera och föreslå vilka bestämmelser om sanktioner som Sverige behöver införa.

Direktivet hindrar inte medlemsstaterna från att anta mer långtgående bestämmelser om säkerhet i nätverk och informationssystem än vad direktivet kräver. Det innehåller även bestämmelser om frivillig rapportering av incidenter. Utredaren får lämna andra förslag denne anser nödvändiga och som ligger inom ramen för EU-direktivet eller dessa direktiv.

Medför direktivet behov av förändringar i sekretesskyddet?

Operatörer som bedriver samhällsviktig verksamhet och leverantörer av digitala tjänster är enligt direktivet skyldiga att

bl.a. anmäla it-incidenter. Som tidigare nämnts bör sådana it-incidenter rapporteras till MSB som får ansvar för Sveriges CSIRT-verksamhet och, i förekommande fall, till aktuell sektorsmyndighet. Därigenom kan aktörerna behöva lämna känslig information om bl.a. säkerhets- och bevakningsåtgärder till tillsynsmyndigheten. En skyldighet att anmäla it-incidenter införs den 1 april 2016 för statliga myndigheter genom en ny bestämmelse i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Den information som statliga myndigheter kommer att rapportera till MSB omfattas av sekretess enligt 18 kap. 8 § 3 offentlighets- och sekretesslagen (OSL) om uppgifterna lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser telekommunikation eller system för automatiserad behandling av information. Det bör analyseras om det finns behov av bestämmelser om sekretessbrytande uppgiftsskyldighet för att berörda myndigheter ska kunna uppfylla sin rapporteringsskyldighet till MSB.

Bestämmelsen i 18 kap. 8 § 3 OSL är utrustad med ett s.k. rakt skaderekvisit. Vid införandet förordade dock flera remissinstanser i stället ett omvänt skaderekvisit (prop. 2003/04:92 s. 78 f.). I samband med att betänkandet Informations- och cybersäkerhet i Sverige (SOU 2015:23) remitterades pekade flera remissinstanser på att sekretesskyddet för aktuella uppgifter behöver ses över. MSB framförde i det sammanhanget att det kan finnas anledning att överväga möjligheten att föreskriva om absolut sekretess för it-incidentrapporter. Det bör analyseras om det nuvarande sekretesskyddet är tillräckligt för att skydda de uppgifter som ska rapporteras till MSB och övriga tillsynsmyndigheter eller om det finns behov av ett starkare sekretesskydd. Uppgifter kan även vara känsliga med hänsyn till den rapporterande aktörens ekonomiska verksamhet. Det bör även analyseras om det befintliga sekretesskyddet för uppgifter om enskilds affärs- och driftsförhållanden är tillräckligt.

Direktivets bestämmelser om samarbete mellan medlemsstaterna kan innebära att information som helt eller delvis omfattas av sekretess behöver utlämnas till annan medlemsstat eller kommissionen. En förutsättning för ett sådant utlämnande är enligt 8 kap. 3 § OSL att utlämnande görs i enlighet med särskilda föreskrifter i lag eller förordning, eller att uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen.

Som nämnts ovan ges medlemsstaterna enligt direktivet möjlighet att skydda information som gäller nationell säkerhet eller som kan påverka möjligheten att upprätthålla lag och ordning särskilt i fråga om brottsbekämpning. Det innebär att Sverige behåller rätten att själv besluta om information som skyddas av sekretess enligt t.ex. 15 kap. 1 och 2 §§ OSL ska delas med andra medlemsstater eller om så inte ska ske. Motsvarande nationell beslutanderätt finns dock inte beträffande sådana uppgifter som endast omfattas av sekretess enligt 18 kap. 8 § 3 OSL. I dag finns ingen särskild föreskrift i lag eller förordning som medger utlämnande av information om it-incidenter till annan medlemsstat eller kommissionen. Det bör övervägas om det finns behov av sådana föreskrifter eller om sådana uppgiftsutbyten som följer av direktivet kan göras med stöd av 8 kap. 3 § första stycket 1 OSL, utan att information som rör rikets säkerhet lämnas ut.

En annan fråga som aktualiseras genom det aktuella direktivet är hur bestämmelserna i en svensk författning om säkerhet i nätverk och informationssystem kommer att förhålla sig till personuppgiftslagstiftningen. Enligt direktivet ska detta inte påverka tillämpningen av dataskyddsdirektivet 95/46/EG, vilket har genomförts i svensk rätt huvudsakligen genom personuppgiftslagen (1998:204). Inom kort förväntas EU besluta om en förordning som utgör en ny generell reglering för personuppgiftsbehandling inom EU. Förordningen kommer att ersätta det nuvarande dataskyddsdirektivet och innebär att bl.a. personuppgiftslagen måste upphävas. Det behöver därför också

analyseras vilken personuppgiftsbehandling som direktivet kan komma ge upphov till och om det medför behov av författningsändringar.

Utredaren ska därför

- ta ställning till om bestämmelserna i offentlighets- och sekretesslagen innebär ett tillräckligt skydd för sådana uppgifter som kan komma att rapporteras med anledning av en it-incident eller om nuvarande lagstiftning behöver ändras och vid sådant behov föreslå författningsändringar,
- undersöka om det behövs en uppgiftsskyldighet för att uppgifter som följer av direktivet ska kunna delas mellan de svenska aktörer som träffas av direktivet och MSB och vid behov föreslå författningsändringar,
- ta ställning till behovet av författningsändringar för att möjliggöra utbyte av andra uppgifter än sådana som rör rikets säkerhet med andra medlemsstater och kommissionen och vid behov föreslå sådana ändringar, och
- analysera vilken personuppgiftsbehandling som kan bli aktuell vid tillämpningen av direktivets bestämmelser och vid behov föreslå författningsändringar.

Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för enskilda och det allmänna samt konsekvenserna i övrigt av förslagen. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras. I 14 kap. 3 § regeringsformen anges att en inskränkning av den kommunala självstyrelsen inte bör gå utöver vad som är nödvändigt med hänsyn till ändamålen. Det innebär att en proportionalitetsprövning ska göras under lagstiftningsprocessen. Om något av förslagen i betänkandet påverkar det kommunala självstyret ska därför, utöver dess konsekvenser, också de särskilda avvägningar som lett fram till förslagen särskilt redovisas.

Arbetets bedrivande och redovisning av uppdraget

Utredaren ska löpande hålla Regeringskansliet (Justitiedepartementet) informerat om arbetet.

Vid genomförandet av uppdraget ska utredaren hålla sig informerad om arbetet med betänkandena Informations- och cybersäkerhet i Sverige (SOU 2015:23) och En ny säkerhetsskyddslag (SOU 2015:25). Utredaren ska också hålla sig informerad om det arbete som bedrivs i Dricksvattenutredningen (L 2013:02) och av den utredare som bistår Justitiedepartementet med att utreda frågan om åtgärder för att öka Polismyndighetens tillgång till information om itbrottslighet.

Under genomförandet av uppdraget ska utredaren, i den utsträckning som bedöms lämplig, också ha en dialog med och inhämta upplysningar från de myndigheter och andra organisationer som berörs av aktuella frågor.

Uppdraget ska redovisas senast den 1 maj 2017.

(Justitiedepartementet)