Dokumentklass:	Öppen
Datum:	2016-12-23
Version:	1.0

Delrapport:
Gemensamma säkerhetskrav

- Som stöd för kravställning vid upphandling

Representanter från kommuner

SOES ska verka för att enskilda individer, företag och det allmänna ska ha tillgång till och förtroende för att:

- samhällets betalningar* fungerar och
- systemen för att betala varor och tjänster fungerar

Syftet är att förebygga allvarliga störningar för att minska konsekvenser av händelser som kan få allvarliga samhällspåverkande effekter.

Detta sker genom att ur ett samhällsperspektiv analysera risk och sårbarhet för kritiska resurser samt beroenden, dokumentera dessa, ta fram förslag för åtgärder, och tillställa ansvariga aktörer.

* *Med samhällets betalningar menas hela kedjan från generering av underlag för utbetalning till att mottagaren kan använda medlen. I målet ingår delar som de olika aktörerna inte har ett direkt ansvar för, men där avbrott påverkar mottagaren menligt. Exempel på detta är aktörer inom finansiella sektorn, för dessa gäller att SOES analyserar och informerar om risker.*

Sammanfattning

För SOES-myndigheternas förmåga att genomföra samhällsviktiga betalningar föreligger flera ömsesidiga och myndighetsgemensamma beroenden. Avbrott vid en enskild myndighet eller vid en enskild leverantör kan därmed påverka flera myndigheters verksamhet, samt betalningsprocesserna i dess helhet i en förlängning. I detta sammanhang kan myndighetsgemensam kravställning gentemot externa leverantörer avseende säkerhetskrav verka robusthetshöjande för såväl de enskilda myndigheterna som för betalningsprocesserna i stort.

Gemensamma säkerhetskrav kan handla om kravställning inom en rad olika områden och för en rad olika tjänster. Säkerhetskrav kan betraktas utifrån olika perspektiv och kan därför variera mellan olika verksamheter och olika verksamhetsområden. Kravställningen kan avse både den egna verksamheten eller verksamhet utanför den egna organisationen och kan därför tillämpas på såväl interna som externa resurser. Genom att inhämta information om myndigheternas syn på möjligheter och utmaningar med formande av gemensamma säkerhetskrav är ambitionen att identifiera hur en gemensam lägstanivå avseende säkerhetskrav kan uppnås.

Fastställande av gemensamma säkerhetskrav och identifierande av en gemensam lägstanivå innefattar utmaningar till följd av att myndigheterna vanligen har olika behov och att kravställning bör anpassas utifrån dessa vid varje givet upphandlingstillfälle. De säkerhetskrav som ställs kan också variera mellan myndigheter och inom de enskilda myndigheterna gentemot olika delverksamheter. De möjligheter som identifierats består bland annat av en gemensam lägstanivå bland leverantörer, där lika krav väntas bidra till förhöjd lägstanivå på marknaden. Gemensamma säkerhetskrav anses också, i och med myndigheternas ömsesidiga beroende, kunna stärka hela processkedjan. Användning av ramavtal är ett exempel på gemensam lägstanivå som redan finns i dagsläget.

Säkerhetsskyddad upphandling (SUA) är ett område där myndigheterna skulle kunna identifiera gemensamma säkerhetskrav, i form av gemensamma principer och åtgärder eller en gemensam lägstanivå. Myndigheterna delar delvis samma utmaningar och erfarenheter, och de grundläggande lagkraven är desamma för alla SOES-myndigheter när uppdrag omfattas av säkerhetsskyddslagstiftningen. Därför kan samarbete och erfarenhetsdelning stärka de enskilda myndigheternas SUA-arbete, vilket i förlängningen även kan stärka myndighetsgemensamma processer.

Mot bakgrund av ovan föreslås att SOES-myndigheterna fortsätter verka för att kravställningsarbetet stärks i processens samtliga steg, såväl inför upphandling som under uppdrag och vid avslut av avtal. Inom ramen för SOES arbete föreslås att framtida aktiviteter fortsatt bör främja erfarenhetsdelning. Exempel på aktiviteter som föreslås inkluderar workshops och seminarier med fokus på kravställning, men även utveckling av vägledningar och annat stödmaterial, såsom mallar och checklistor.

Innehåll

1 Inledning

Syftet med denna rapport är att genom fördjupade analyser avseende gemensamma säkerhetskrav, bygga vidare på tidigare arbete för stärkt kravställning och på så sätt öka medvetenheten om hur gemensamma säkerhetskrav kan bidra till stärkt robusthet och stärkta samhällsbetalningar i en förlängning. Genom att inhämta information om myndigheternas syn på möjligheter och utmaningar med formande av gemensamma säkerhetskrav är ambitionen att identifiera hur en gemensam lägstanivå avseende säkerhetskrav kan uppnås.

1.1 Bakgrund

Samverkansområde Ekonomisk säkerhet (SOES) arbetar för att enskilda individer, företag och det allmänna ska ha tillgång till - och förtroende för - samhällets betalningar samt att systemen för att betala varor och tjänster fungerar. Verksamheten inom SOES har därmed till uppgift att förebygga allvarliga störningar i betalningssystemet och att minska konsekvenser av händelser som kan få allvarliga samhällspåverkande effekter.

SOES Arbetsgrupp Analys (AG Analys) har sedan 2013 arbetat med att identifiera, analysera och ge förslag till robusthetshöjande åtgärder för stärkta samhällsbetalningar. Flera av de analyser som genomförts har fokuserats till myndighetsgemensamma beroenden, såsom beroende till leverantörer för tillförsel av bl.a. el, IT-drift och elektronisk kommunikation.[1] En utmaning med ett högt myndighetsgemensamt beroende till externa leverantörer som lyfts fram i tidigare rapporter består i minskade möjligheter för SOES-myndigheterna att styra och upprätthålla sin kritiska verksamhet. Som förslag till robusthetshöjande åtgärder har bland annat en ändamålsenlig och effektiv kravställning gentemot leverantörer lyfts fram samt gemensamma säkerhetskrav för stärkt kravställning inom bland annat IT-säkerhetsområdet. Under 2015 fördjupades tidigare analys av externa beroenden utifrån ett kravställningsperspektiv. Denna rapport kompletterar tidigare genomförda studier med att analysera gemensamma säkerhetskrav som underlag för stärkt kravställning, med uppgift att identifiera en gemensam lägstanivå avseende säkerhetskrav.

1.2 Syfte och mål

Syftet med denna rapport är att öka SOES-myndigheternas förståelse av hur gemensamma säkerhetskrav bland myndigheter kan bidra till stärkt robusthet samt stärkta samhällsbetalningar i en förlängning.

Målet med denna fördjupning är att analysera gemensamma säkerhetskrav som underlag för stärkt kravställning, med ambitionen att utifrån övergripande och gemensamma erfarenheter identifiera hur en gemensam lägstanivå avseende säkerhetskrav kan uppnås.

---

[1] SOES (2013) *Samhällskonsekvensanalys för myndigheterna inom SOES*

Den huvudsakliga målgruppen för denna rapport är personer inom SOES-myndigheterna som på ett eller annat sätt arbetar med inköp och upphandling, men även de personer som på annat sätt har ett intresse för kravställning.

1.3 Ingångsvärden och avgränsningar

Tidigare studier avseende robusthetshöjande åtgärder har utgjort huvudsakliga ingångsvärden till studien. Det myndighetsgemensamma beroendet till leverantörer där myndigheterna delvis delar samma utmaningar och erfarenheter har varit särskilt betydande, tillsammans med identifierade förslag till robusthetshöjande åtgärder i form av gemensamma säkerhetskrav.

Denna rapport gör varken anspråk på att ge någon heltäckande beskrivning avseende myndigheternas befintliga säkerhetskrav eller att ge någon uttömmande beskrivning av de erfarenheter som omnämnts vid intervjuer och workshops.

1.4 Metod

Referensmaterial till denna studie bygger på en skrivbordsstudie, en intervjustudie och två workshops. Intervjustudien har insamlat myndigheternas syn på möjligheter och utmaningar med att identifiera gemensamma säkerhetskrav och en gemensam lägstanivå för desamma för att ge förslag till hur gemsamma säkerhetskrav och en gemensam lägstanivå kan uppnås. Intervjuerna har även insamlat goda exempel på kravställning genom upphandlingens alla faser. Skrivbordsstudien har inventerat relevant referensmaterial på området kravställning, medan den inledande workshopen fokuserades till att identifiera utmaningar och möjligheter med att fastställa gemensamma säkerhetskrav. Den avslutande workshopen har fokuserats till säkerhetsskyddad upphandling, som exempel på ett område för gemensamma säkerhetskrav och en gemensam lägstanivå.

En förteckning av genomförda intervjuer och en deltagarförteckning över genomförda workshops återfinns i bilaga 1.

2 Myndighetsgemensamma säkerhetskrav

Säkerhetskrav kan handla om alltifrån fysisk säkerhet i form av skalskydd till informationssäkerhetsfrågor. Gemensamma säkerhetskrav kan på så sätt handla om kravställning inom en rad olika områden och för en rad olika tjänster. Säkerhetskrav kan betraktas utifrån olika perspektiv och kan därför variera mellan olika verksamheter och olika verksamhetsområden. Kravställningen kan avse krav för den egna verksamheten eller för verksamhet utanför den egna organisationen och kan därför tillämpas på såväl interna som externa resurser.

Myndigheterna i Sverige är självständiga, vilket medför att varje enskild myndighet fastställer säkerhetskrav för dess egen verksamhet utifrån de lagar och regler som är gällande. På samma sätt bedriver myndigheterna dess eget upphandlingsarbete, med grund i identifierat behov inom egen verksamhet. Sett utifrån ett SOES-perspektiv föreligger samtidigt ömsesidiga- och myndighetsgemensamma beroenden för genomförande av samhällsviktiga betalningsprocesser. Avbrott vid en enskild myndighet eller vid en enskild leverantör kan därmed påverka flera myndigheters verksamhet, samt betalningsprocesserna i dess helhet i en förlängning. I detta sammanhang kan myndighetsgemensam kravställning gentemot externa leverantörer avseende säkerhetskrav verka robusthetshöjande för såväl de enskilda myndigheterna som för betalningsprocesserna i stort.

Detta kapitel belyser myndigheternas syn på möjligheter och utmaningar med fastställande av gemensamma säkerhetskrav och identifiering av en gemensam lägstanivå för desamma. Kapitlet innehåller även goda exempel på hur myndigheterna kan verka för gemensamma säkerhetskrav och en gemensam lägstanivå.

2.1 Utmaningar och möjligheter

Bland utmaningarna för gemensam kravställning gentemot externa aktörer betonas att myndigheterna vanligen har olika behov, där ställda krav behöver anpassas utifrån identifierat behov vid varje givet upphandlingstillfälle. Exempelvis kan en myndighet vara i behov av att ställa specifika krav avseende skalskydd för en viss tjänst, medan en annan myndighet inte har identifierat samma behov vid upphandling av en jämförbar tjänst. Ställda säkerhetskrav kan också variera mellan myndigheter och de enskilda myndigheterna kan också ha olikt ställda säkerhetskrav internt gentemot olika delverksamheter.

Möjligheterna med fastställda gemensamma säkerhetskrav beskrivs i sin tur utgöras av en gemensam lägstanivå bland leverantörer, där lika ställda krav kan bidra till att harmonisera och höja lägstanivån på marknaden. Vidare, och på grund av att myndigheterna vanligen har ett ömsesidigt beroende till varandras processer och resurser, ses gemensamma säkerhetskrav kunna stärka hela processkedjan.

Exempel på en gemensam lägstanivå avseende säkerhetskrav som beskrivs finnas idag är användningen av ramavtal. Vissa myndigheter framhåller härvid att säkerhetskraven inom ramen för gällande ramavtal skulle kunna skärpas ytterligare, medan andra upplever att ambitionsnivån redan idag är högt ställd. Förslag till hur myndigheter kan verka för gemensamma säkerhetskrav utgörs bland annat av erfarenhetsutbyte och myndighetssamverkan. Förslag avseende vilken grad av samverkan som bör ske

varierar dock mellan de intervjuade myndigheterna. Flertalet av de personer som har deltagit i intervjustudien efterfrågar utökad samverkan mellan myndigheter, både kring hur gemensamma säkerhetskrav kan utformas men också hur myndigheter på bästa sätt kan dela goda exempel med varandra. Att arrangera myndighetsgemensamma forum för dialog och erfarenhetsutbyte inom specifika områden beskrivs härvid som önskvärt. Utbyte av information via myndighetsgemensamma digitala kunskapsbanker eller gemensamma lagringsytor lyfts därtill fram som en framgångsfaktor.

Exempel på praktiskt stöd för upphandling av varor och tjänster som är kritiska för SOES-myndigheternas identifierade samhällsviktiga betalningsprocesser utgörs av vägledningen *Robusta upphandlingar*.[2] Ett annat stöd är FSPOS vägledning för outsourcad verksamhet.[3]

2.2 Gemensam lägstanivå genom myndighetssamverkan

Vid intervjuerna lyfts samverkan vid kravställning gentemot externa aktörer fram som det enskilt vanligaste förslaget på hur gemensamma säkerhetskrav kan uppnås. Ett första steg till detta beskrivs vara att myndigheterna självmant samverkar i en eller flera delar av upphandlingsprocessen. Samverkan beskrivs här bestå utav informationsdelning och erfarenhetsutbyte mellan funktioner inom olika verksamhetsområden på de olika myndigheterna.

Enligt intervjuade myndigheter finns viss samverkan mellan myndigheter redan idag, vilket beskrivs vara mycket uppskattat av samtliga medverkande parter. Exempel på myndighetssamverkan som nämns är upprättade nätverk mellan myndigheter, där exempelvis Riksgälden har ett nätverk tillsammans med Riksbanken och Finansinspektionen.

> *”Vi berör allt som handlar om upphandling och försöker även hitta områden där vi kan upphandla tillsammans. Vi stämmer av hur vi jobbar och om det finns olikheter i hur de olika myndigheterna jobbar. Att lära av varandra är det viktigaste. Alla myndigheter har egna fokusområden. Att veta hur olika myndigheter arbetar är bra, så kan man dra nytta av och tillämpa vissa delar i det egna arbetet.”*
> *Riksgälden*

Ett annat exempel som nämns är myndighetssamverkan vid enskilda delar av upphandlingsprocessen.

> *”Vi pratar med varandra och har ett samarbete där vi lyssnar på varandras erfarenheter. CSN har vi haft en konkurrenspräglad dialog med under 3 år.”*
> *Försäkringskassan*

[2] MSB (2014) Robusta upphandlingar: Delrapport 1 - Ett delprojekt inom ramen för genomförande av Handlingsplan för skydd av samhällsviktig verksamhet

[3] *Appendix G Kontinuitetshantering för outsourcad verksamhet* i FSPOS (2015) *Vägledning för kontinuitetshantering*.

Utmaningen med varför ett tydligt samverkansarbete inte alltid har inletts menar flera beror på resursbrist och tidsbrist. En stark sammanhållande part identifieras också som viktig för att åstadkomma kontinuitet i samverkansarbetet.

> *”Ju mer man kan enas och samköra, desto bättre tror jag. Inte bara för myndigheterna utan även för leverantörerna. Jag tror mer på ett standardiserat förfarande. I allas intresse. Det behövs en tydlig part som håller i det hela. Nu har vi SOES som diskuterar upphandlingar, men det är svårt att få till ett driv, säkert på grund av tidsbrist.”*
> *MSB*

För stärkt myndighetssamverkan efterfrågas bland annat tydligare stöd och vägledning avseende specifika områden, exempelvis säkerhetsskyddad upphandling. Forum för kontinuerlig dialog och erfarenhetsutbyte efterfrågas särskilt. En framgångsfaktor i detta sammanhang beskrivs bestå av ett brett deltagande av myndigheter samt representation i form av olika kompetenser. För det senare har det exempelvis lyfts fram att vana upphandlare kan lära av de som är relativt nya på området och vice versa. Några myndigheter efterfrågar upprättade nätverk för dialog om kravställning mellan myndigheter, samtidigt som utmaningen med att avsätta tid och resurser omnämns. Myndigheterna framhåller också vikten av att ha en sammanhållande part i ett sådant nätverk. En gemensam lagringsyta lyfts fram som ytterligare en del i att underlätta informationsdelningen mellan SOES-myndigheter.

2.3 Goda exempel genom upphandlingens faser

Ett förslag till hur myndigheterna kan verka för gemensamma säkerhetskrav som omnämnts är att dela goda exempel mellan myndigheter. Att arbeta på liknande sätt – och ta stöd av goda exempel från varandra – beskrivs därmed som ett sätt att arbeta för en höjd gemensam lägstanivå. Sett till upphandlingens faser finns ett antal förhållningssätt som omnämnts som särskilt viktiga för framgångsrik(a) enskilda- och myndighetsgemensamma upphandlingsprocesser.

Innan en upphandling

Merparten av arbetet kring en upphandling utförs i en inledande fas. Förberedelser i form av planering och utformning av förfrågningsunderlag är ramverket som ska hålla samman upphandlingen från start till mål. Ett utökat informationsutbyte i inledningsfasen mellan myndigheter med likartade behov har lyfts fram som en nödvändighet och framgångsfaktor för att identifiera en gemensam lägstanivå avseende säkerhetskrav. Understödjande faktorer som nämns är att tillgängliggöra information och mallar i en kunskapsbank samt att dela informationen genom befintliga nätverk för erfarenhetsutbyte.

Gör en marknads- och behovsanalys

Flera intervjupersoner understryker vikten av att ta sig tid att göra en gedigen förstudie med analys av det egna behovet och tillgängligt utbud på marknaden innan en upphandling inleds. Behovsidentifieringen kan här ses vägledande för den senare kravställningen gentemot leverantören. Utmaningar som nämns är att förstudier till en början kan tyckas onödiga samt att arbetet kräver omfattande resurser. Samtidigt framhåller flertalet att en gedigen förstudie sparar både tid och resurser i slutändan.

”Ett konkret tips är att göra sin förstudie och våga prata med marknaden. Det kan ibland finnas en rädsla för att prata med marknaden - men det är där kompetensen finns.”
Skatteverket

”En gedigen förstudie tjänar man på i slutändan.”
Kammarkollegiet

Säkerställ rätt kompetens

Enligt myndigheterna är det viktigt att involvera rätt funktioner redan vid det inledande skedet av upphandlingen. Identifierat behov bör vara styrande för vilken kompetens och vilka roller som ska involveras i upphandlingsarbetet. Vanligen bör representanter från följande verksamheter inkluderas i upphandlingsarbetet redan i det inledande skedet: verksamheten (beställaren), upphandlingskompetens (inköpsavdelning eller motsvarande), säkerhetsavdelningen och IT.

”Samarbeta. Försök att hitta tvärfunktionella grupper för att effektivisera. Personal inom säkerhet och verksamhet måste ha kompetensen att kunna upphandla.”
Skatteverket

”Ansvariga kravställare från verksamheten är alltid med. När upphandlingen berör IT-system så finns även lämpliga resurser från IT med i upphandlingen.”
Riksgälden

”Vi bedriver förvaltningsområdesorganiserade upphandlingar, vilket innebär att det är avdelningarna som äskar resurser så att man säkerställer tillgång till rätt kunskap.”
Pensionsmyndigheten

En utmaning för framför allt mindre myndigheter är att ha personal med upphandlingskompetens internt. En framgångsfaktor som lyfts fram är att ta in extern kompetens.

”Vi är en relativt stor myndighet och har förmånen att kunna fråga om hjälp med kravställning inom IT in house. Är man är en liten myndighet så måste man kanske ta in en konsult för den typen av tjänster.”
PTS

Säkerhetsskydd eller inte

När behoven är identifierade och upphandlingskompetensen är på plats är nästa steg att bestämma vilket upphandlingsförfarande som är tillämpligt. Innan myndigheten beslutar om vilket förfarande som ska tillämpas ska myndigheten avgöra om upphandlingen bör säkerhetsskyddas eller inte. Flera SOES-myndigheter hanterar ofta information som kan behöva säkerhetsskyddas. Om upphandlingen ska omfattas av säkerhetsskydd måste myndigheten ta fram ett skriftligt säkerhetsskyddsavtal innan affärsavtalet tas fram.

”Man måste direkt, innan själva upphandlingen startar ställa sig frågan ”finns det någon aspekt i upphandlingen eller uppgifter i uppdraget som är säkerhetsskyddad?”. I så fall ska det vara en SUA.”
Statens Servicecenter

I intervjustudien efterfrågas mer stöd och vägledning kring hur myndigheter på bästa sätt genomför en säkerhetsskyddad upphandling.

”Vi har relativt nyligen börjat med SUA-upphandlingar, så vi är nybörjare. I och med planeringen för civilt försvar så har detta blivit ännu mer aktuellt för oss. Det vi gör är att prata med Säpo och Fortifikationsverket, men vi söker även tips och råd från andra myndigheter som vi tror har mer erfarenhet av SUA-upphandlingar än vad vi har.”
PTS

Om upphandlingen inte ska SUA-klassas kan myndigheten gå vidare och identifiera vilka andra upphandlingsförfaranden som kan komma i fråga.

Lär känna marknaden

Dialogen med leverantörer bedöms som en utmaning men även som en framgångsfaktor när den bedrivs på ett effektivt och framgångsrikt sätt. Denna dialog är viktig under hela kravställningsprocessen och är därför relevant redan vid formulering av behov och vid utformningen av förfrågningsunderlag. De flesta myndigheter rekommenderar att ta kontakt med marknaden innan upphandlingen startar. Kammarkollegiet tipsar även om att ta kontakt med alla de olika branschorganisationer som finns och som ofta har bred kunskap om olika ämnen.

Att som beställande myndighet använda sig av RFI (Request For Information) anges av några intervjupersoner som en framgångsfaktor. Genom användande av RFI:er, kan beställaren ges ingångsvärden av marknadens kunskap och erfarenheter, för att därigenom kunna skapa ett marknadsanpassat förfrågningsunderlag som även uppfyller myndighetens behov. Därutöver ges tillfälle för leverantörerna att så tidigt som möjligt i processen lämna synpunkter och ställa frågor som de anser är av betydelse för upphandlingen.

”Det är bättre med dialog och dra nytta av leverantörernas kunnande inom området.”
Försäkringskassan

”Ett råd är att träffa leverantörerna och undersök vad som finns på marknaden.”
PTS

”Det är bra för att få grepp om vilka aktörer som finns och få en känsla för vad marknaden har att erbjuda, för att bygga kunskap innan en upphandling.”
Statens Servicecenter

”Vi vill ha större flexibilitet hos leverantören och även se till att få in nytt folk i branschen. Vi tror att det finns duktiga människor som

> *inte har 8 års erfarenhet av konsultrollen till exempel. Vi beskriver istället arbetets svårighetsgrad och därefter får leverantörerna föreslå resurser samt vilken stöd eller hjälp resurserna behöver för att kunna leverera.”*
> *Försäkringskassan*

Samtidigt är det viktigt att poängtera att för de flesta upphandlingar ska all dialog med leverantörerna ske innan upphandlingen startar. Ibland lyfts en oro kring att prata med marknaden utifall det skulle ses som en konkurrensfördel för vissa leverantörer. Det har tidigare använts som skäl för att inte ha kontakt med marknaden, vilket kan leda till att upphandlingen inte blir lika framgångsrik som den hade kunnat vara. Ett antal av intervjupersonerna menar att det är en gammal föreställning som lever kvar hos en del myndigheter och som bygger på en rädsla av att bryta mot regelverket. Det är fullt tillåtet, och rekommenderas av bland annat Upphandlingsmyndigheten och Kammarkollegiet, att ha en dialog med leverantörerna innan upphandlingen startar.

> *”Många är rädda för att använda RFI. Om man ber dem prata med en leverantör så blir de bekymrade. Här på Kammarkollegiet uppmanar vi dem att ha en dialog innan, då man får prata om vad som helst. Vi rekommenderar det!”*
> *Kammarkollegiet*

En utmaning med att ha en dialog med leverantörerna är att det är tidskrävande.

> *”Det finns alltid ett stort tryck på behovet av att ha en dialog med leverantörerna, men det är inte så lätt i praktiken. Ofta handlar det om tidspress. Jag tror att man som upphandlare inte har tid att ha den relationen med leverantörer som man kan behöva. Särskilt i ett inledande skede.”*
> *MSB*

Konkretisera tillämpliga kvalificerings- och säkerhetskrav

Det sista och slutgiltiga steget i förberedelsefasen handlar om att sammanställa kvalificeringskrav och säkerhetskrav. Även vid utformande av kvalificeringskrav bör säkerhetskrav beaktas. För utformande av säkerhetskrav kan myndighetens egna risk- och kontinuitetsanalyser vara bra att använda för att omsätta de egna behoven till konkreta krav. De kan ofta ge svar på vad leverantörer bör uppfylla, exempelvis på tjänsters tillgänglighet och robusthet, men även på prioriteringen av krav. Ett tips är att göra listor där alla krav sedan rankas i prioriteringsordning. Det finns ett antal generiska krav som kan användas vid upphandling och som kan utgöra en utgångspunkt för gemensam kravställning gentemot externa leverantörer. Hos Kammarkollegiet finns en rad stödmaterial som kan vara vägledande vid kravställningsarbetet, bland annat dokumentation avseende basnivå avseende säkerhetskrav vid outsourcing. För enskilda myndigheter kan exempelvis krav ställas på kontinuitetsplaner hos leverantörer. Kravställningen kan även innefatta särskilda krav på exempelvis kompetens, service och tillgänglighet eller andra tekniska krav. Vägledande bör här vara de interna krav som myndigheten har och dess eget kontinuitetsarbete.

Flera myndigheter lyfter fram att de områden som är svårast att kravställa kring handlar om ”mjuka värden”, som till exempel miljökrav och sociala krav. Dessa krav

beskrivs även som svåra att följa upp. Det är också viktigt att få med underleverantörerna i kravställningen, så att de krav som gäller för huvudleverantören även gäller för eventuella underleverantörer.

> *”Miljörelaterade, liksom etiska och sociala krav är kan vara svåra att ställa men framför allt att följa upp. En aktuell fråga är möjligheten att ställa krav på kollektivavtalsliknande villkor och hur dessa krav ska formuleras.”*
> *Kammarkollegiet*

> *”Inom IT-säkerhet finns mycket vägledning och folk i branschen. När det gäller informationssäkerhet handlar det om mer processer som kan vara svårt att kravställa kring. Det förutsätter att rätt kompetens finns.”*
> *Skatteverket*

Myndigheterna lyfter även fram att det finns en utmaning avseende att hitta rätt balans i kravställningen och att samtidigt kunna motivera kostnaden.

> *”Vi har SLA på alla nivåer. Speciellt när det gäller tillgänglighetstider och avbrottstider. Men det är svårt att hitta rätt typ av nyckeltal och få det till att passa prislappen. Vad är en rimlig nivå?”*
> *Statens Servicecenter*

> *”Balansen är svår, vilket också stärker nyttan med djupa förstudier. Varje ändring som görs kostar ju också mer pengar, så ju mer man kan komma tillrätta med från början desto bättre.”*
> *Pensionsmyndigheten*

> *”Kompabilitet kan vara svårt. Ofta när man köper något ska det in i något annat system. Att formulera det på ett bra och öppet sätt är inte alltid lätt. Avtalsvillkor kan också vara svårt att hamna på rätt nivå.”*
> *MSB*

En annan aspekt som är viktig att ta hänsyn till är teknikutvecklingen. Alltför snäva tekniska krav kan leda till att möjligheterna och fördelarna med ny teknik omöjliggörs. De flesta myndigheter har som ambition att ställa funktionella krav framför tekniska krav, vilken innebär leverantören besvarar ”hur” kravet ska uppfyllas, istället för att myndigheten uppger tekniska detaljer avseende hur lösningen ska upprättas.

> *”Vi har tidigare gått på en del minor genom att vi har ställt för detaljerade tekniska krav. Då är det inte alldeles enkelt att uppfylla dem. Till exempel har vi kravställt runt datacenter. Leverantörerna hade säkert kunnat göra detta på ett bättre sätt om vi hade ställt funktionskrav istället.”*
> *Försäkringskassan*

> *”Man säger ju alltid att man vill jobba med funktionella krav. Jag tror att man inte riktigt kan ha koll på alla lösningar som finns tillgängligt, och att man därför inte vågar ställa för specifika krav. Upphandlingarna ska inte vara för riktade. Det jag har sett genom*

åren är att allt för tekniska krav kostar pengar.”
MSB

”Funktionalitetskrav är sådant som alla pratar om, men i regel hamnar man ändå bland mutter och skruv till slut.”
Pensionsmyndigheten

Under och efter

Efter att varan/tjänsten har levererats har myndigheten ett arbete i att följa upp sina avtal och leveranser samt utvärdera utfallet. Krav som ställs bör vara tydliga, rimliga och mätbara så att de kan följas upp. Det bör samtidigt beaktas att uppföljning är resurskrävande och förenligt med kostnader. Höga tillgänglighetskrav och hög robusthet kan vara kostsamt, i synnerhet om redundansen är högre än nödvändigt.

Uppföljning

Att följa upp ställda krav anses av ett flertal intervjupersoner som en utmaning. Uppföljningen upplevs av flera myndigheter som tidskrävande och svårt. Om tjänsten levereras utan incidenter, hamnar ofta uppföljningen av säkerhetskraven i skymundan. Hur uppföljningen går till är olika på respektive myndighet. En del använder sig av egna checklistor eller någon annan form av stöd för uppföljning, medan andra lämnar uppföljningen åt respektive avdelning att följa upp på egen hand.

”Jag har ett IT-stöd för att följa upp. Det kommer påminnelser om att prata med beställare och prata med leverantören. Får vi det vi har beställt, till det pris vi har kommit överens om?”
PTS

”Det är ett utmanande arbete att följa upp de krav man har ställt. Formerna har inte riktigt satt sig ännu. Huvudregeln är att om det fungerar bra, så är det tyst från beställar-sidan.”
”Men vi försöker att följa upp kontinuerligt. Vi har en tydlig och noga avtalsleverantörsuppföljningsplan inom IT-området, där leverantörerna klassas på en skala.”
Pensionsmyndigheten

”Alla fleråriga avtal har en utsedd avtalsförvaltare som ansvarar för att följa upp avtalet. Uppföljningen är inte alltid dokumenterad.”
Riksgälden

”Jag tror att myndigheterna har tillräckligt med att ställa kraven. När det sedan gäller att följa upp löpande är det vanligt att det brister. Det är först när det händer något som man går in och undersöker vad som hänt.”
Statens Servicecenter

Konsensus råder kring att ”mjukare värden” är svårare att följa upp. Det kan till exempel gälla miljökrav eller sociala krav. Dessa krav är också de som anses svårast att kravställa kring i upphandlingen.

”Vi ställer krav på etiska krav innan upphandling, men det är svårt att följa upp hur det de facto går till i ett senare skede.”
Kammarkollegiet

För stöd vid avtalsuppföljning finns en vägledning som framtagits av Kammarkollegiet.[4]

[4] Kammarkollegiet(2011) *Kontraktsuppföljning – säkerställ goda affärer genom att följa upp.*

3 Gemensamma säkerhetskrav för säkerhetsskyddad upphandling (SUA)

Vid intervjuer med representanter för SOES-myndigheterna har säkerhetsskyddad upphandling (SUA) nämnts som ett område där myndigheterna skulle kunna identifiera gemensamma säkerhetskrav, i form av gemensamma principer och åtgärder eller en gemensam lägstanivå. I detta kapitel redovisas en analys av hur gemensamma säkerhetskrav skulle kunna utvecklas för myndigheternas arbete med säkerhetsskyddad upphandling. Analysen är dels baserad på en skrivbordsstudie av tillgängliga vägledningar och stöd kopplat till myndigheters SUA-tillämpning, dels på diskussioner vid en workshop med såväl SOES-myndigheter som ett antal andra myndigheter.

3.1 Varför gemensamma säkerhetskrav för SUA?

Liksom all kravställning, behöver säkerhetsskyddet anpassas till varje berörd myndighet och dess verksamhet. Tillämpningen av SUA sker utifrån enskilda myndigheters behov, men också utifrån deras egen erfarenhet och tolkning. Myndigheterna delar samtidigt delvis samma utmaningar och erfarenheter och de grundläggande lagkraven är desamma för alla SOES-myndigheter när uppdrag omfattas av säkerhetsskyddslagstiftningen. Flera myndigheter ser SUA som något utmanande, exempelvis när SUA bör användas och hur kravställningen kopplat till SUA bör upprättas och följas upp.

Flera delar av tillämpningen av SUA upplevs som öppen för tolkning av berörda SOES-myndigheter och vissa myndigheter har mer erfarenhet av SUA än andra. Det har därför poängterats att mognadsnivån och angreppssättet gällande SUA skiljer sig åt SOES-myndigheterna emellan. Samarbete och erfarenhetsdelning kan därför stärka de enskilda myndigheternas SUA-arbete, vilket i förlängningen även kan stärka myndighetsgemensamma processer.

3.2 Vad är SUA?

Säkerhetsskydd innebär att myndigheter och andra som säkerhetsskyddslagstiftningen gäller för ska vidta förebyggande åtgärder mot brott som kan hota rikets säkerhet, såsom spionerі och sabotage. När det i en upphandling förekommer uppgifter som med hänsyn till *rikets säkerhet* omfattas av sekretess (*hemliga uppgifter*) har staten, kommuner och landsting ansvaret för att det finns ett fullgott säkerhetsskydd hos leverantören. Myndighetens hemliga uppgifter ska ges samma säkerhetsskydd hos anbudsgivare och leverantör som de har på myndigheten. Myndigheten ska då träffa ett skriftligt avtal – ett säkerhetsskyddsavtal – med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det enskilda fallet. Denna process benämns säkerhetsskyddad upphandling (SUA).[5] [6] Om förfrågningsunderlaget innehåller

[5] SÄPO (2010), *Säkerhetsskyddad upphandling – En vägledning*, sid 5-6, 10.

[6] Enligt 8 § säkerhetsskyddslagen gäller att: *”När en myndighet upphandlar, där det i förfrågningsunderlaget eller under uppdragets utförande förekommer hemliga uppgifter eller där leverantören kommer att delta i verksamhet med betydelse för rikets säkerhet, ska ett*

hemliga uppgifter innebär det att ett säkerhetsskyddsavtal måste tecknas redan innan anbudsgivaren kan få del av förfrågningsunderlaget.

> *”Ett säkerhetsskyddsavtal innebär att säkerhetsskyddsåtgärder vidtas hos en leverantör för att säkerställa att uppgifter som omfattas av sekretess med hänsyn till rikets säkerhet hanteras på ett säkert sätt. Därför är det av största vikt att processen med säkerhetsskyddad upphandling går rätt till”*
> SÄPO, *Säkerhetsskyddad Upphandling – en vägledning*

Kraven på myndigheter att upprätta SUA styrs framförallt av *säkerhetsskyddslagen (1996:627)* och *säkerhetsskyddsförordningen (1996:633)*. Säkerhetsskyddsförordningen ställer bland annat krav på att myndigheter genomföra en säkerhetsanalys, där man undersöker vilka uppgifter i verksamheten som skall hållas hemliga med hänsyn till rikets säkerhet och vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism.[7] Säkerhetspolisen (SÄPO) har också tagit fram en vägledning till handläggning av säkerhetsskyddad upphandling, som är styrande för hur myndigheter tillämpar SUA.[8] I vägledningen beskrivs bland annat den övergripande processen för handläggning av SUA, men även beskrivning av de delar som behöver ingå i arbetet. Bland annat ställs inför avtal särskilda krav på en säkerhetsbedömning, att leverantören upprättar en säkerhetsskyddsinstruktion för de skyddsåtgärder den ska vidta, att leverantörens personal säkerhetsprövas och registerkontrolleras med stöd av SÄPO, samt att myndigheten gör ett besök hos leverantören för att kontrollera lokal m.m. Därutöver ställs krav på fortlöpande utbildning och tillsyn hos leverantören under uppdraget.

3.3 Vilket stöd och vägledning finns för tillämpning av SUA?

SÄPO:s vägledning för handläggning av SUA beskriver som sagt den övergripande processen och dess respektive delar. I några avsnitt ges praktiska exempel på särskilda sakfrågor att beakta i tillämpningen. Vägledningen innehåller även mallar för säkerhetsskyddsavtal. Samtidigt har myndigheterna poängterat att vägledningen i större utsträckning innehåller *vad* som ingår i SUA-arbetet men i mindre utsträckning *hur* tillämpningen går till. En inventering har därför gjorts av öppna källor med andra aktörers stöd och exempel som ett komplement till de krav som presenteras i SÄPO:s vägledning. Tabellen nedan följer processen som den beskrivs i Säpos vägledning. Relevant kompletterande information som har identifierats hos andra myndigheter finns noterade kolumnen till höger.

Del av SUA	Kommentar från Säpos vägledning	Stöd/exempel från andra aktörer
Säkerhetsanalys	Utifrån Myndighetens generella säkerhetsanalys bör myndigheten göra en analys av det uppdrag som är	Från Svenska Kraftnäts hemsida: • ”Checklista inför säkerhetsanalys” • ”Checklista inför riskanalys”

säkerhetsskyddsavtal upprättas med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs”

[7] *5 § Säkerhetsskyddsförordning (1996:633)*

[8] SÄPO (2010), *Säkerhetsskyddad upphandling – En vägledning*.

	aktuellt för upphandling.	
Säkerhetsplan	Resultatet av den för uppdraget genomförda analysen bör dokumenteras i en säkerhetsplan	Från Svenska Kraftnät (via energisäkerhetsportalen): • ”Checklista för säkerhetsmässig kravställning” Från FMV: • ”Industrisäkerhetsmanual” – ”Rubrikindelning för säkerhetsskyddsplan”
Säkerhetsbedömning	Säkerhetsplan utgör underlag för bedömning om ett säkerhetsskyddsavtal ska träffas	Från FMV: • ”Industrisäkerhetsmanual” – Underlag för säkerhets-skydd/Säkerhetsskyddsplan”
Val av upphandlings-form	Upphandling som rör rikets säkerhet regleras i 15 kap. LOU och LUF. En upphandling enligt 15 kap. LOU och LUF ska göras genom förenklat förfarande eller urvalsförfarande. I vissa fall får också direktupphandling användas.	Från Konkurrensverket: • ”Upphandlingsreglerna - en introduktion”
Säkerhetsskyddsavtal	I säkerhetsskyddsavtalet, som ska vara skriftligt, regleras vilka säkerhetsskyddsåtgärder som ska vidtas i den aktuella upphandlingen.	Från Fortifikationsverkets hemsida: • ”Checklista för SUA” Från Svenska Kraftnät (via energisäkerhetsportalen): • ”Checklista SUA” + registerkontroll Från SÄPO:s vägledning: • ”Mall säkerhetsskyddsavtal” (nivå 1-3)
Säkerhetsskydds-instruktion	Av leverantören upprättade bestämmelser eller arbetsordning för hur säkerhetsskyddet med hänsyn till kontrakterat SUA-uppdrag ska bedrivas inom företaget. Säkerhetsskyddsinstruktionen och förändringar i den ska alltid godkännas av den beställande myndigheten. I de fall företaget ska utföra arbete i myndighetens lokaler eller i lokaler som har anvisats av myndigheten (säkerhetsskyddsavtal nivå 2 och 3) får myndigheten medge att en säkerhetsskyddsinstruktion inte behöver upprättas	Från Försvarsmakten: • ”Handbok Säkerhetsskyddad upphandling med säkerhetsskyddsavtal” - Bilaga 5 Exempel på disposition av säkerhetsskyddsinstruktion - Bilaga 6 Exempel på säkerhetsskyddsinstruktion”
Underrättelse till Säpo	En myndighet ska utan dröjsmål underrätta Säkerhetspolisen om säkerhetsskyddsavtal som har träffats	
Säkerhetsprövning av ledning och styrelse	Innan myndigheten lämnar ut hemliga uppgifter till ett företag ska myndigheten göra en säkerhetsprövning och, om uppdraget är placerat i säkerhetsklass, låta göra en	Från Fortifikationsverkets hemsida: • ”Lathund för Säkerhetsprövning” • ”Bedömningsgrunder vid säkerhetsprövning” • ”Mall för samtycke om

	registerkontroll av företagets ledning.	registerkontroll” Från Svenska Kraftnät: • Checklista SUA + registerkontroll
Sekretessförbindelse	Myndigheten ska också se till att en sekretessförbindelse undertecknas	Från Fortifikationsverkets hemsida: • ”Mall för sekretessförbindelse”
Förstagångsbesök	Om hemliga uppgifter ska lämnas ut till ett företag som ska hantera och förvara uppgifterna i egna lokaler, ska myndigheten genomföra ett besök hos företaget.	Från FMV: • ”Industrisäkerhetsmanual” – Bilaga 8 Underlag för genomförande av säkerhetsrevision)”
Säkerhetsprövning av övriga i uppdraget	När affärsavtalet har träffats ska säkerhetsprövning och, om uppdraget är placerat i säkerhetsklass, registerkontroll ske av övriga anställda på företaget som ska delta i uppdraget och som kan antas komma att få del av hemliga uppgifter	Från Försvarsmakten: • ”Handbok för Försvarsmaktens säkerhetstjänst, Säkerhetsprövning” • ”Handbok Säkerhetsskyddad upphandling med säkerhetsskyddsavtal” - Bilaga 2 Mall för säkerhetsprövning” Från FMV: • ”Industrisäkerhetsmanual” – Bilaga 8 Dokumenterad personbedömning)”
Utbildning	Utbildningen med syfte att klargöra varför skyddsåtgärder ska vidtas mot hot av olika slag ska genomföras, samt säkerställa att behörig personal har tillräcklig kunskap rörande säkerhetsskyddet i det aktuella uppdraget.	
Tillsyn	Företaget bör fortlöpande kontrollera att endast behöriga personer deltar i uppdraget, att åtgärderna i säkerhetsskyddsavtalet och säkerhetsskyddsinstruktionen vidtas Myndigheten ska kontrollera att företaget har vidtagit de avtalade säkerhetsskyddshöjande åtgärderna och genomfört en säkerhetsskyddsutbildning med de personer som kommer att få del av hemliga uppgifter i uppdraget. Denna kontroll kan om myndigheten önskar genomföras i samråd med Säkerhetspolisen och/eller Försvarsmakten.	Från Svenska Kraftnät: • ”Checklista för egenkontroll” Från Försvarsmakten: • ”Försvarsmakten - Handbok Säkerhetsskydd - Bilaga 7 Lathund för kontroll/ tillsyn av ett företag med säkerhetsskyddsavtal nivå 1”
Säkerhetsskyddsavtalet sägs upp	När uppdraget är fullfört	
Underrättelse till SÄPO	SÄPO underrättas om att säkerhetsskyddsavtalet har upphört att gälla	
Avanmälan av registerkontroll	Samtliga registerkontroller som är kopplade till uppdraget avanmäls	

3.4 Möjliga gemensamma säkerhetskrav för SUA?

Vid en workshop diskuterades möjliga gemensamma säkerhetskrav kopplat till myndigheternas tillämpning av SUA. Vid workshopen deltog representanter från ett flertal SOES-myndigheter men även från Post- och Telestyrelsen (PTS), Statens servicecenter och Transportstyrelsen. Deltagarna diskuterade inledningsvis ett antal styrkor och utmaningar med SUA, därefter ett antal mer specifika frågor om tillämpning och uppföljning.

Avslutningsvis identifierades ett antal förslag till åtgärder för att höja den gemensamma lägstanivån avseende myndigheternas arbete med SUA. Flera av dessa förslag kan betraktas som gemensamma säkerhetskrav, i form av förslag till gemensamma tillvägagångssätt baserat på myndigheternas respektive erfarenheter. Samarbete och erfarenhetsdelning skulle därmed kunna stärka de enskilda myndigheternas SUA-arbete, vilket i förlängningen även kan stärka myndigheternas gemensamma kravställning i form av SUA.

Styrkor och utmaningar med SUA-arbetet

Enligt myndigheterna handlar styrkorna med SUA framförallt om nyttan av det förebyggande arbetet i sig, men också om trygghetsskapande och de signaler SUA medför såväl inom myndigheten som externt mot leverantörer och allmänhet. De identifierade styrkorna återges i nedanstående tabell.

Vilka är de största styrkorna med SUA?	
Förebyggande säkerhetsskyddsarbete	**Trygghets- och förtroendeskapande**
Bidrar till att förebygga och minimera risker kopplat till säkerhetsskyddet i de uppdrag som berörs	Lyfter vikten av säkerhetsskyddsfrågan och ger ett ökat fokus på säkerhetsskydd, såväl inom myndigheterna som externt
Ger tillgång till en ”verktygslåda” av säkerhetsskyddsåtgärder, t.ex. registerkontroll med hjälp från SÄPO	Skapar en trygghet för myndigheterna genom att man får kontroll på leverantörerna och deras personal. SUA fungerar på så vis som en kvalitetsstämpel på utförande av uppdraget.
Fungerar som ett kvitto på att man är överens med leverantören om vad som gäller	Medför en trygghet för medborgarna om att myndigheterna gör rätt för sig

Ett flertal utmaningar för myndigheternas SUA-arbete har identifierats. Dessa gäller generellt att arbetet medför omfattande administration och hur man ska förhålla sig till upphandlingslagstiftning. Ett antal mer specifika utmaningar noterades även gällande SUA-kravställningen mot leverantörer inför och under ett avtal. Därutöver diskuterades delar i SUA-processen som myndigheterna upplever som otydliga eller öppna för tolkning. Dessa utmaningar berör i hög utsträckning den inriktning och vägledning om SUA som finns tillgänglig från lagstiftning och från SÄPO. De identifierade utmaningarna återges i nedanstående tabell.

Vilka är de främsta utmaningarna i arbetet med SUA?		
Generella utmaningar	**Kravställning mot leverantör**	**Otydligheter i process och tillämpning**
Generellt mer utmanande med Säkerhetsnivå 1, pga. fler och högre krav på leverantören	Utmanande att få leverantörer att inse vad SUA-kraven innebär. Ibland bekräftar leverantörer att de uppfyller	Bedömning av vad som ska omfattas av SUA och tolkning av begreppet ”rikets säkerhet”, även om det är tydligt att

	kraven men att det sedan visar sig att detta inte är fallet	bedömningen ska utgå ifrån myndighetens säkerhetsanalys
Stor intern administration, bl.a. manuellt arbete med mallar och att samma leverantör behöver ett SUA-avtal per uppdrag	Utmanande att skapa tydlighet mot leverantören att deras SUA-relaterade arbete ska ingå i priset för leverans (t.ex. leverantörens egen administration och säkerhetsskyddsåtgärder)	Möjlighet att upprätta SUA i förväg utan ett specifikt uppdrag/avrop? – T.ex. med avtal med flera leverantörer och förnyad konkurrensutsättning. Vissa har fått OK från SÄPO om detta, andra har fått ett tydligt NEJ
Utmanande att förhålla sig till proportionalitetsprincipen som gäller för upphandlingsregler, t.ex. i LOU	Uppföljning mot leverantörer, i synnerhet mot konsulter som arbetar från egen lokal	Hur LOU och LUF används är otydligt i SÄPO:s vägledning (som innehåller vissa inaktuella uppgifter och bygger på regler innan LUFS fanns).
Hantering av underleverantörsavtal, såväl mängden underleverantörer som insyn hos dessa aktörer	Hantering av avtal mellan myndigheter, då man inte får kontrollera andra myndigheters medarbetare. Säkerhetsskyddet är då beroende av att den andra myndigheten genomför kontrollen	SÄPO ger ibland tvetydiga svar eller olika svar beroende på vem på SÄPO man frågar

Erfarenheter avseende beslut om och planering inför upprättande av SUA

Vid workshopen diskuterades ett antal mer specifika frågor om deltagarnas erfarenhet avseende beslut om och planering inför upprättande av SUA. Vid diskussionen konstaterades att vissa av myndigheterna har stor erfarenhet av SUA och har en mer utarbetad process för tillämpningen. Andra myndigheter har haft relativt mindre erfarenhet och har därför upprättat mindre rutiner och färre mallar, m.m. Erfarenhetsdelningen identifierade ett flertal goda exempel, som myndigheterna kan ta med sig i sina respektive organisationers tillämpning av SUA. Därutöver nämndes även exempel på myndigheters egna mallar som kan delas med övriga deltagare. De identifierade erfarenheterna återges i nedanstående tabell.

Erfarenheter avseende beslut om och planering inför upprättande av SUA	
Bedömning av om SUA-avtal bör ingå i kravställningen	Det kan konstateras att det finns en skillnad i erfarenhet av SUA mellan myndigheterna Vissa, med större erfarenhet, har ett mer formaliserat angreppsätt: • Upphandlingsprocess med formell beslutspunkt om SUA • Fördefinierad säkerhetsanalys av myndighetens system och information som underlag för beslut • Checklistor och frågeformulär finns på plats som stöd • Upphandlare/inköp tar stöd av säkerhetsavdelningen. Vid beslut om SUA Andra, har relativt mindre erfarenhet, har ett mindre fördefinierat förhållningssätt: • SUA inkluderas inte alltid som en förbestämd och formell beslutspunkt i upphandlingsförfarandet • Förfarandet mer personberoende, t.ex. huruvida beställare har erfarenhet av SUA-beslut och säkerhetsanalys • Checklistor och frågeformulär inte alltid på plats och säkerhetsanalys inte alltid lättillgänglig

	• Beslut utgår från en i dialog mellan upphandlare/inköp och säkerhetsavdelningen
Goda exempel på upprättande av säkerhetsanalys och säkerhetsplan	Några utgångspunkter som nämndes av myndigheterna: • Utgå från SÄPOs processflöde (i *Säkerhetsskyddad upphandling – En vägledning*) • Använd experter i egna organisationen som hjälp i analysen: - Samarbeta med controllers och med de som arbetar med RSA inom myndigheten. Den kommande, nya, säkerhetsskyddslagen kräver en säkerhetsskyddsplan (säkerhetsskyddsanalys), vilket också ger en tydligare koppling mot RSA - Samverkan mellan säkerhetsskyddschef och IT-säkerhetschef underlättar analysarbetet - Underlag till analysen kan bl.a. inhämtas genom workshops och intervjuer • Tänk på att säkerhetsplanen bör innehålla en tidsplan och åtgärdslista • Tänk på att hålla analysen separerad från öppna nät och att den endast är tillgänglig för behöriga
Goda exempel på hur säkerhetsskyddschef kan samverka med inköp/upphandlare	Följande erfarenheter nämndes av myndigheterna: • Planera gemensamt med inköp och säkerhetsavdelningen i hela upphandlingsförfarandet. Tänk på att ha framförhållning i arbetet, bl.a. då det finns ledtider att förhålla sig till • Använd och dela tillgängliga manualer/checklistor, såväl egna som andras • Ta fram och arbeta utifrån gemensamma styrande dokument. Arbeta utifrån en tydlig och väl kommunicerad säkerhetsanalys • Säkerhetsavdelningen behöver vara tillgängliga och ge stöd, t.ex. till upphandlare/inköp.
Bedömning huruvida sekretessavtal ska tecknas med leverantörens personal i uppdrag som omfattas av säkerhetsskyddsavtal	Myndigheten, eller den som myndigheten bestämmer, ska upplysa berörda personer om: • Innebörden och räckvidden av den tystnadsplikt som gäller för de hemliga uppgifterna i uppdraget • Eventuella föreskrifter i säkerhetsskyddsinstruktionen • Innebörden av begreppet behörig • Straffbestämmelserna i 19 kap. brottsbalken avseende brott mot rikets säkerhet. Myndigheten ska också se till att en sekretessförbindelse undertecknas. Undertecknande av sekretessförbindelse är en skriftlig bekräftelse på att uppdragstagaren har informerats om innebörden av tystnadsplikten och säkerhetsskyddet.
Förslag på kompletteringar i SUA-avtal, utöver SÄPO:s standardtexter	Myndigheterna använder och uppskattar de standardtexter som finns men välkomnar ytterligare standarder och exempel. I några fall finns bland myndigheterna erfarenhet från egna kompletteringar. Specifika tillägg i avtal kan vara lämpliga, t.ex. så att det framgår om uppdraget inkluderar underleverantör eller särskilda tillägg om fysiskt skydd (insynsskydd, inpassering etc. vilket kan vara relevant ffa för SUA nivå 1) För att dra nytta av varandras erfarenhet, nämndes av deltagarna att myndigheterna delar dessa avtalsmallar med varandra framöver.

Erfarenheter avseende uppföljning och tillsyn av SUA

Liksom diskussionen om beslut om och upprättande av SUA, resonerade myndigheterna även kring ett antal specifika frågor om erfarenhet avseende uppföljning och tillsyn av SUA. Även inom detta område identifierades ett flertal goda exempel och mallar, exempelvis gällande säkerhetsskyddsinstruktion och frågor vid förstagångsbesök. De identifierade erfarenheterna återges i nedanstående tabell.

Erfarenheter avseende uppföljning och tillsyn av SUA	
Uppföljning av innehållet i SUA-avtalet upp som en del av kravställningen	Följande erfarenheter nämndes av myndigheterna: • Satsa på ett nära samarbete mellan upphandlare/inköp (den som äger avtalet) och säkerhetsavdelningen • Strukturerad leverantörsstyrning är en viktig framgångsfaktor. För särskilt kritiska leverantörer (t.ex. nivå 1), kan ett särskilt säkerhetsråd upprättas • Skicka ut kontrollfrågor till leverantörer om hur de följer upp delarna i avtalet. Därutöver genomförs även kontrollbesök • En rimlig lägstanivå för uppföljning bör vara minst årligen
Goda exempel kring begäran om uppgifter och leverantörens säkerhetsskyddsinstruktion	Instruktionen är en viktig del i att förklara betydelsen av säkerhetsskyddet. Enligt myndigheterna så finns en avsevärd skillnad i mognad och erfarenhet mellan leverantörerna gällande detta område. Vissa har stor vana och har egna exempel, vissa saknar erfarenhet och har inte tagit fram en säkerhetsskyddsinstruktion tidigare. Myndigheterna lyfte fram följande goda exempel från det egna arbetet: • Det är viktigt att vara transparenta med säkerhetsskyddskraven från början och att från början klargöra att anbudsgivare diskvalificeras om det visar sig att man inte uppfyller kraven med sin säkerhetsskydds-instruktion • Flera av myndigheterna har egna mallar för säkerhetsskyddsinstruktion. Myndigheten kan förse leverantören kan med mallar/exempel rörande säkerhetsskyddsinstruktionen. Leverantören är ofta positiv till detta, i synnerhet om den saknar erfarenhet av SUA, då det kan underlätta processen • En generisk mall är bra att utgå ifrån, men måste kompletteras och anpassas utifrån hur leverantören möter kraven
Goda exempel på kontrollfrågor vid förstagångsbesök	Följande exempel nämndes av myndigheterna: • Polisen har ett frågebatteri och uppsatta principer att utgå ifrån vid förstagångsbesök. • För vissa uppdrag kan det vara viktigt att komma ihåg kravställning som beaktar krav på obligatorisk IT-incidentrapportering ned till krav på leverantören • mot bakgrund av kraven i *MSBFS 2016:2 föreskrifter och allmänna råd om statliga myndigheters rapportering av IT-incidenter* samt i *säkerhetsskyddsförordningen* • Det är viktigt att ställa frågor och krav som är konkreta/specifika, t.ex. rutin för och tidskrav på incidentrapportering till myndigheten

I vilken utsträckning kan/bör myndigheten ta stöd av SÄPO och/eller Försvarsmakten vid uppföljning?	Civila myndigheter tar eventuellt stöd från SÄPO. Flera av myndigheterna har erfarenhet av dialog med SÄPO om stöd: • SÄPO har begränsade resurser för att stötta och det finns erfarenhet av att man har fått nej vid förfrågan om stöd vid förstagångsbesök. Bedömningsvis är det svårt både att få stöd vid besök och med mail-/telestöd, men kan gå om man hittar rätt person och är ute i god tid • Det finns en önskan bland myndigheterna stöd från SÄPO med ytterligare mallar, exempelvis i linje med det som de som finns från Polisen för frågor vid förstagångsbesök
Goda exempel på internkontroll av SUA	Flera av myndigheter konstaterar att det finns ett utvecklingsbehov med att etablera internkontroll för SUA, t.ex. gällande utbildning.

Gemensamma säkerhetskrav avseende SUA

Det framgår tydligt av analysen att det finns skillnader mellan myndigheternas erfarenhet och arbetssätt med SUA, och att det är en utmaning att etablera en gemensam lägstanivå. Tillämpningen av säkerhetsskyddad upphandling kommer även fortsättningsvis att anpassas till varje berörd myndighet och dess verksamhet. Samtidigt delar myndigheterna många utmaningar från SUA-arbetet och de grundläggande lagkraven är desamma. Ett sätt att närma sig gemensamma säkerhetskrav avseende SUA har därför varit att dela erfarenheter mellan myndigheter. Kan exempelvis handla om att en myndighet har hittat en lösning på en annan myndighets utmaning genom att redan ha formulerat rätt frågeställningar eller tagit fram en ändamålsenlig mall.

En annan typ av gemensamma säkerhetskrav som framträder ur diskussionerna är behovet av klargörande av otydliga områden och frågor som berör SUA. Flera av dessa frågor kan tydliggöras genom dialog mellan myndigheterna, men i flera fall efterfrågas även ytterligare förklaring och stöd från SÄPO. En gemensam dialog med SÄPO skulle underlätta en mer enhetlig tillämpning av SUA, vilket i förlängningen kan främja utvecklingen av gemensamma säkerhetskrav. Ett flertal specifika förslag, som skulle kunna höja lägstanivån och utgöra en del av gemensamma säkerhetskrav inom dessa områden, har framförts av myndigheterna:

Erfarenhetsdelning och förbättring i myndigheters SUA-arbete:

- Myndigheterna drar nytta av befintliga vägledningar, t.ex. från SÄPO, FMV, Försvarsmakten, Svenska Kraftnät, Fortifikationsverket, m.fl.
- Myndigheterna delar, återanvänder och inför checklistor, mallar, frågebatteri och goda exempel (såväl egna som från andra aktörer)
- Myndigheterna inför en formell beslutspunkt om SUA i sin upphandlingsprocess, om detta saknas
- Myndigheterna genomför uppföljning av leverantörer med SUA-avtal minst årligen
- Myndigheterna integrerar, när detta är möjligt, SUA-arbetet med RSA och intern styrning och kontroll, t.ex. genom gemensam process och gemensamma workshops när analyser genomförs
- Myndigheterna för en gemensam dialog med SÄPO, både utanför SOES och inom ramen för SOES-arbete (t.ex. i form av överlämning av resultat från workshopen och ev. framtida workshops, utbildningar, eller annan samverkan där SÄPO deltar)

Förbättringar i SUA-processen som sådan och behov av stöd/inriktning från SÄPO:

- Kan SÄPO ge tydligare förhållningsregler och riktlinjer?
- Kan SÄPO utveckla ytterligare mallar och exempel som stöd till myndigheterna, t.ex. i form av case med ”Exempelmyndigheten” där tillämpning beskrivs?
- Kan SÄPO tydligare koppla/strukturera vägledningen enligt ISO 27002?
- Kan ett IT-verktyg utvecklas för registerkontroll, för att undvika manuell hantering/administration?
- Kan SÄPO ge en samlad bild och dra slutsatser om identifierade utmaningar, behov och förbättringsbehov kopplat till SUA (t.ex. behov av utbildning, bättre säkerhetsanalyser, mer frekvent uppföljning m.m)?
- Kan SÄPO ge mer enhetliga svar/råd där ”samma fråga får samma svar”?

4 Avslutande kommentarer

Denna rapport har påvisat att det finns en rad utmaningar och möjligheter med att fastställa gemensamma säkerhetskrav och att identifiera en gemensam lägstanivå avseende säkerhetskrav för myndigheter. Utmaningar som lyfts fram är att myndigheterna är självständigt upphandlande myndigheter och att behov kan variera mellan myndigheter. Möjligheter som lyfts fram är en höjd lägstanivå avseende säkerhetskrav på marknaden.

Förslag till hur gemensamma säkerhetskrav och en gemensam lägstanivå kan uppnås har i intervjusvaren främst fokuserats till informations- och erfarenhetsdelning och kravställning utifrån ett processperspektiv, snarare än specifika krav avseende exempelvis skalskydd eller informationssäkerhet. För att ge en mer heltäckande bild avseende möjliga gemensamma säkerhetskrav eller en gemensam lägstanivå kan en mer grundlig studie göras med fokus på exempelvis fysiskt skydd eller informationssäkerhetsskydd. Samtidigt kan informations- och erfarenhetsdelning och en myndighetssam process för säkerhetskravställning möjligen ses stärka de enskilda myndigheternas upphandlingsprocesser avseende att ställa merändamålsenliga krav, vilket kan stärka samhällsbetalningarna i en förlängning.

5 Nästa steg

Målsättningen med denna rapport har varit att utifrån övergripande och gemensamma erfarenheter bland SOES-myndigheter identifiera hur en gemensam lägstanivå avseende säkerhetskrav kan uppnås. Tidigare kapitel har presenterat intervjuade myndigheters syn på utmaningar och möjligheter för hur gemensamma säkerhetskrav och en gemensam lägstanivå för säkerhetskrav kan uppnås. Nedan sammanfattas ett antal förslag till fortsatt arbete inom och utanför SOES.

5.1 Förslag till fortsatt arbete inom SOES

SOES-myndigheterna föreslås verka för att kravställningsarbetet stärks i processens samtliga steg, såväl inför upphandling som under uppdrag och vid avslut av avtal. Kravställningsprocessen kan bland annat stärkas genom att myndigheterna delar erfarenheter och exempel med varandra, såsom mallar, checklistor och processbeskrivningar. Erfarenhetsdelningen bör emellertid inte begränsas till SOES-myndigheterna, utan kan även omfatta utbyte med andra myndigheter, då krav på myndigheter och utmaningar gällande kravställning ofta är samma eller snarlika för andra myndigheter. Ett sådant område då leverantörer upphandlas och då uppdraget behöver omfattas av säkerhetsskyddad upphandling (SUA). Gällande SUA, och andra tillämpliga områden, bör myndigheterna dela, återanvända och införa befintliga checklistor, mallar, frågebatteri, exempel, m.m. i sin kravställning. Inom ramen för SOES arbete, bör framtida aktiviteter fortsatt främja erfarenhetsdelning och kunskapshöjning. Exempel på aktiviteter kan därför inkludera workshops och seminarier med fokus på kravställning, men även utveckling av vägledningar och annat stödmaterial, såsom mallar och checklistor.

Ett annat sätt för SOES-myndigheterna att stärka kravställningsprocessen är verka för ytterligare stöd och tydlighet när andra aktörer ger inriktning om hur kravställning bör ske. Detta gäller exempelvis när en annan myndighet har ett tillsynsuppdrag över myndigheterna eller har gett ut föreskrifter eller vägledningar kopplat till kravställning. Ett konkret exempel på detta är vägledning från SÄPO gällande säkerhetsskyddad upphandling. SOES-myndigheterna bör föra en gemensam dialog med SÄPO, eller i andra tillämpliga fall, om myndigheternas behov av stöd, vägledning och förtydliganden. Exempel på aktiviteter skulle detta fall kunna vara att bjuda in SÄPO till en gemensam workshop eller att gemensamt efterfråga mallar, exempel, svar på otydliga frågor eller utbildning. Genom att gemensamt föra denna dialog ges emfas till behoven och förmågehöjande aktiviteter kan effektiviseras.

5.2 Förslag till fortsatt arbete för annan aktör

Ett konkret behov har identifierats hos myndigheterna att få ytterligare stöd från SÄPO gällande säkerhetsskyddad upphandling. SÄPO föreslås beakta de utmaningar och behov som har identifierats i denna rapport och överväga myndigheternas förslag. Några av dessa beaktanden är mer generella, exempelvis att myndigheterna efterfrågar tydligare förhållningsregler och riktlinjer gällande SUA från SÄPO. Andra önskemål är mer konkreta, t.ex. huruvida SÄPO kan utveckla ytterligare mallar och exempel som stöd till myndigheterna, t.ex. i form av case med ”Exempelmyndigheten” där tillämpning av SUA beskrivs. Andra sådana önskemål är om SÄPO kan göra en tydligare koppling av SUA-vägledning enligt ISO 27002 och huruvida ett IT-verktyg

skulle kunna utvecklas för registerkontroll, för att undvika manuell hantering och administration.

Referenslista

Appendix G Kontinuitetshantering för outsourcad verksamhet i FSPOS (2015) *Vägledning för kontinuitetshantering*.

Kammarkollegiet(2011) *Kontraktsuppföljning – säkerställ goda affärer genom att följa upp.*

MSB (2014) Robusta upphandlingar: Delrapport 1 - Ett delprojekt inom ramen för genomförande av Handlingsplan för skydd av samhällsviktig verksamhet

SOES (2013) *Samhällskonsekvensanalys för myndigheterna inom SOES*

Säkerhetsskyddsförordning (1996:633)

SÄPO (2010), *Säkerhetsskyddad upphandling – En vägledning.*