Avdelningen för säker kommunikation

# Sammanställning och analys av inkomna remissvar avseende ändring av PTS föreskrifter om krav på driftsäkerhet

## 1 Inledning

Post- och telestyrelsen (PTS) har den 17 oktober 2019 skickat ut ett förslag till ändring av föreskrifter på remiss som innehåller förslag på ytterligare krav på driftsäkerhet för den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster (nedan tillhandahållare). Remisstiden gick ut den 14 november 2019.

Nedan sammanställs de huvudsakliga synpunkter som framförts i inkomna remissvar, tillsammans med PTS inställning till remissinstansernas synpunkter.

## 2 Inkomna remissvar

PTS har tagit emot remissvar från följande myndigheter, operatörer och övriga organisationer och företag: AB Stokab, AB Svenska Bostäder, Hi3G Access AB, Huawei Technonolgies Sweden AB, Infobip Sweden AB, Konkurrens-verket, Myndigheten för samhällsskydd och beredskap, Polismyndigheten, ServaNet AB, Svenska kraftnät, Svenska Stadsnätsföreningen, Sveriges kommuner och landsting, Säkerhetspolisen, Tele2 Sverige AB, Telenor Sverige AB och Telia Company AB.

### 2.1 Remissinstanser utan synpunkter på de föreslagna ändringarna

AB Svenska Bostäder, Infobip Sweden AB, Konkurrensverket, Svenska kraftnät och Sveriges kommuner och landsting har inga synpunkter på de föreslagna ändringarna.

Polismyndigheten tillstyrker förslaget till ändring av de aktuella föreskrifterna.

AB Stokab har inget att erinra mot de föreslagna ändringarna som nu är föremål för remiss, men framför synpunkter rörande rimligheten i de krav som uppställs på reservkraft i de befintliga föreskrifterna.

*PTS kommentar:*

*PTS kommenterar inte de synpunkter som inkommit på de redan idag beslutade och gällande kraven på driftsäkerhet. Det kommer dock ske en revidering av samtliga föreskriftskrav om skyddsåtgärder under 2020.*

# 3 Övergripande kommentarer

## 3.1 Allmänt om krav på driftsäkerhet

Hi3G Access AB framför att alla tillhandahållare måste se till att kommunikationsnäten är robusta och säkra, idag och framöver, annars kommer kunderna av konkurrensskäl vända sig till andra tillhandahållare. Driftsäkerhet är således centralt för Hi3G Access AB och något som bolaget jobbar kontinuerligt med.

Tele2 Sverige AB delar PTS ambition att främja tillgången till säkra och effektiva elektroniska kommunikationer och välkomnar därför i stort förslaget till ändring.

Huawei Technologies Sweden AB välkomnar den allmänna riktningen som PTS tar genom att med en riskbaserad metod hantera driftsäkerhet.

Svenska Stadsnätsföreningen anser att det är bra att föreskrifterna kontinuerligt ses över, och att det är bra för branschen att de finns.

ServaNet AB ser i allmänhet positivt på de av myndigheten föreslagna ändringarna.

AB Stokab ser positivt på att PTS utfärdat föreskrifter för att klargöra kraven på god driftsäkerhet.

Säkerhetspolisen ser positivt på att PTS reviderar de befintliga driftsäkerhets-föreskrifterna och delar PTS uppfattning om att de finns risker relaterade till den kommande utbyggnaden av 5G och risker förknippade med att samhället blir alltmer beroende av säkra elektroniska kommunikationer.

Telia Company AB anser i huvudsak att de åtgärder som PTS föreslår i grunden är bra och nödvändiga.

Telenor Sverige AB ser överlag positivt på stärkt fokus på driftsäkerhet och bedömer att de nya kraven inte medför någon större förändring jämfört med hur operatören redan idag arbetar med driftsäkerhet.

*PTS kommentar:*

*PTS ser mycket positivt på det generella bemötandet av skärpningen av kraven på driftsäkerhet. Myndigheten kan konstatera att i stort samtliga remissinstanser delar PTS uppfattning att ytterligare krav på driftsäkerhet är nödvändiga.*

*När det gäller kommentaren att marknadens aktörer tillhandahåller robusta och säkra nät för att inte kunderna ska vända sig till andra tillhandahållare, vill PTS framföra att myndighetens erfarenhet är att tillhandahållare många gånger vidtar skyddsåtgärder av kommersiella skäl, och att dessa skyddsåtgärder till och med många gånger kan gå utöver vad som krävs för att uppnå den rimliga nivån av driftsäkerhet som lagen kräver. Dock har PTS också många gånger genom tillsyn erfarit att skyddsåtgärder som vidtagits endast av kommersiella hänsyn inte varit tillräckliga sett till ett samhälleligt perspektiv, varför det är nödvändigt att säkerställa en grundläggande nivå av säkerhet som garanteras alla användare genom tvingande föreskrifter.*

## 3.2 Kommentarer om krav som inte föreslagits

Framförallt Säkerhetspolisen framför kommentarer om att PTS förslag på ändringar inte är tillräckliga för att säkerställa att syftet uppnås, och hänvisar till de principer som Säkerhetspolisen framfört i sitt remissvar över betänkandet Frekvenser i samhällets tjänst (SOU 2018:92) och promemorian Kompletterande förslag till betänkandet, eftersom man anser att dessa principer bör vara styrande för hur en tillhandahållare bedriver sitt driftsäkerhetsarbete. Säkerhetspolisen framför att man anser att samtliga de principer som lyfts fram ska omhändertas i driftsäkerhetsföreskrifterna.

Vidare framför säkerhetspolisen bl.a. att PTS inte tagit hänsyn till att det kommer att komma en ny lag om elektronisk kommunikation som till viss del ändrar förutsättningarna för föreskrifterna.

*PTS kommentarer:*

*Syftet med de nu aktuella ändringarna har aldrig varit att omhänderta alla de eventuella risker som t.ex. utbyggnaden av 5G förväntas innebära. Snarare har dessa ändringar bedömts hantera en delmängd av riskerna. PTS är medveten om detta och har begränsat ändringarna i förslaget i syfte att i tillräcklig utsträckning hinna utreda kraven och dess konsekvenser, och ta fram rimliga regler inom sådan tid att ändringarna blir relevanta i relation till kommande och pågående utbyggnad.*

*Såsom framgår av konsekvensutredningen kommer PTS att göra om samtliga föreskrifter med grundläggande säkerhetskrav (inklusive nya krav för incidentrapportering till PTS) under 2020, bl.a. som ett led i att anpassa kraven efter de lagändringar som är på gång. De nu aktuella föreskriftsändringarna utgör en liten, men viktig, pusselbit i skapandet av de kommande föreskrifterna om säkerhet.*

*I den utsträckning som det är lämpligt och tidsmässigt möjligt, samt direktiv och lagstiftning på området tillåter, kan PTS komma att beakta de av Säkerhetspolisen lyfta principerna i*

*kommande föreskriftsarbete, men myndigheten anser inte att det är lämpligt att inom ramen för denna mindre revision hantera frågan.*

# 4 Kommentarer på de föreslagna kraven

## 4.1 Att införa ytterligare dokumentationskrav

Hi3G Access AB framför att skyldigheten att ta reda på och dokumentera samtliga tillverkare och uppdragstagare är en mycket omfattande administrativ uppgift och att denna börda bör vägas mot nyttan av en sådan åtgärd.

Säkerhetspolisen ser positivt på att det tas in utökade krav på dokumentation men framför att man vill att dokumentationskravet ska omhänderta samtliga de förhållanden som nämns i av Säkerhetspolisen lyfta styrande principer.

Telenor Sverige AB har förståelse för kraven på dokumentation och framför att det redan är en naturlig del av operatörens säkerhetsarbete.

*PTS kommentar:*

*PTS ser att bördan med att införa ytterligare dokumentationskrav står i proportion till nyttan av att skapa en kontinuerlig och god överblick och spårbarhet över den utrustning och de uppdragstagare som är kopplade till verksamheten.*

*PTS ser inte att det i denna revision är lämpligt att beakta de av Säkerhetspolisen framförda principerna, se ovan.*

### 4.1.1 Dokumentation av tillverkare

Hi3G Access AB anser att det är mycket omfattande och orealistiskt att dokumentera tillverkare, i synnerhet för förbindelser som man hyr. Bolaget efterfrågar även motivering till varför dokumentationen ska sparas i fem år.

Svenska Stadsnätsföreningen önskar klargörande av vem som är tillverkare av en förbindelse när en sådan anläggs. Svenska Stadsnätsföreningen anser att det är rimligt att dokumentationen hålls uppdaterad och bevaras i fem år, men efterfrågar tydliggörande om vad som ska göras med dokumentationen sen.

Myndigheten för samhällsskydd och beredskap framför att ”tillverkare” inte finns definierat i föreskrifterna och att en tillgång kan bestå av flera komponenter med olika tillverkare.

Telia Company AB är tveksamma till att varje version av dokumentationen ska sparas i fem år. Bolaget framför även att kostnaderna för de ökade dokumentationskraven är grovt underskattade.

*PTS kommentarer:*

*När det gäller tillverkare av hyrda förbindelser så anser PTS att en tillhandahållare måste säkerställa att såväl den infrastruktur som man själv äger som den som man hyr lever upp till en rimlig driftsäkerhetsnivå. Som tillhandahållare får man därför åtminstone kravställa att den man hyr ifrån har en dokumentation över förbindelserna som lever upp till kraven, som man har rätt att ta del av.*

*Såsom Svenska Stadsnätsföreningen antagit i sitt remissvar ser PTS också att det är den som tillverkat själva utrustningen som utgör förbindelsens tillverkare. Syftet med kravet på dokumentation är att skapa en spårbarhet över vem som står bakom den utrustning som utgör tillhandahållarens nät eller tjänst. Om det t.ex. skulle framkomma att en viss tillverkares produkter är behäftade med kvalitetsproblem så ska det vara enkelt för en tillhandahållare att snabbt kontrollera och vid behov hantera den utrustning som har dessa problem.*

*När det gäller tillverkare av tillgångar är PTS medvetna om att en tillgång kan utgöras av många enskilda komponenter som i sig kan ha flera olika tillverkare. Såsom framgår av konsekvensutredningen är det upp till tillhandahållaren att själv avgränsa vad som utgör en tillgång, utifrån definitionen av detta i de befintliga reglerna. Av detta följer att det även blir upp till tillhandahållaren att närmare avgöra på vilken nivå man dokumenterar tillverkare.*

*PTS anser att kravet på dokumentation av tillverkare endast är en mindre utvidgning av de krav som redan gäller, samt att tillhandahållare i stor utsträckning redan bedöms ha denna information, varför PTS inte anser att kravet kostnadsmässigt är underskattat. Att spara dokumentationen i fem år anser myndigheten är rimligt sett till att det inte kan uteslutas att det framkommer brister eller sårbarheter i en viss utrustning även efter så lång tid som fem år och att det därför är viktigt med en spårbarhet även bakåt i tiden.*

*När tillhandahållaren inte längre är skyldig att bevara dokumentationen får denna sparas eller gallras efter tillhandahållarens egen bedömning.*

#### 4.1.2 Dokumentation av uppdragstagare

Hi3G Access AB anser att det är en stor administrativ börda att dokumentera samtliga uppdragstagare, samt att definitionen av uppdragstagare är för vid. Operatören föreslår att endast de uppdragstagare som jobbar med kärnnätet ska dokumenteras.

Myndigheten för samhällsskydd och beredskap anser att tillhandahållare även ska dokumentera uppdragstagares organisationsnummer. Myndigheten framför även att det bör framgå att dokumentationen ska sparas i *minst* fem år, dvs. att man kan spara den längre.

Telia Company AB framför att det är självklart att huvudsakliga kontaktuppgifter sparas i samband med kontraktsskrivning, men att det inte alltid finns uppgifter om varje enskild person utför arbete i näten. Telia Company AB anser att kravet bör gälla delar med en utökad risk.

Telenor Sverige AB uppger att uppgifter om bl.a. uppdragstagare och uppdragens omfattning är en naturlig del av operatörens dokumentation.

*PTS kommentarer:*

*PTS anser inte att det är ändamålsenligt att begränsa kravet på dokumentation av uppdragstagare till att endast omfatta vissa delar av näten. Näten och tjänsterna blir aldrig starkare än sin svagaste länk och på det sätt som även mindre noder och tillgångar hänger ihop med överliggande, kritiska punkter, såväl idag som troligen än mer i framtiden, ser PTS att det är nödvändigt och en självklarhet att tillhandahållare har kontroll över vilka uppdragstagare man anlitar i alla delar av näten. PTS ser inte att man kan nå upp till en rimlig nivå av driftsäkerhet utan att tillhandahållare har en överblick och spårbarhet över vilka företag man anlitar att t.ex. utföra underhåll och drift. Den administrativa bördan som detta medför för den tillhandahållare som inte redan har detta dokumenterat idag anser PTS vara proportionerlig i förhållande till risken för avbrott och störningar.*

*PTS föreskrifter om krav på driftsäkerhet och de föreslagna ändringarna av dessa utgör en minimireglering. Det står den tillhandahållare som anser att man behöver vidta ytterligare åtgärder för att säkerställa säkerheten i nät och tjänster fritt att göra så, t.ex. att spara dokumentation längre än vad reglerna kräver. PTS anser inte att detta behöver tydliggöras ytterligare direkt i kraven.*

*PTS håller med Myndigheten om samhällsskydd och beredskap om att det är lämpligt att även ställa krav på att dokumentera organisationsnummer. PTS ändrar således kravet till att även omfatta detta.*

## 4.2 Ytterligare hot i riskanalysen

Telenor Sverige AB framför att sabotage redan idag är en sådan form av yttre påverkan som omfattas av operatörens riskanalyser. Telenor Sverige AB välkomnar även införandet av möjligheten för PTS att informera om hot att beakta i riskanalysen, eftersom relevant information om nya hot och risker alltid läggs till de säkerhetsanalyser som operatören utför och uppdaterar vid behov. Telenor Sverige AB påpekar också vikten av att sådan information är tillräckligt konkret och detaljerad.

Hi3G uppger att man inte har tolkat att hotet ”sabotage” skulle innefattas i ”yttre påverkan”, och ifrågasätter om inte detta snarare är ett hot som hanteras i säkerhetsskyddslagstiftningen och tillsyn av denna. Om hotet ska beaktas i driftsäkerhetsföreskrifterna anser Hi3G Access AB att det endast ska gälla för aktuella och för kritiskt infrastruktur relevanta hotbilder om sabotage.

Även när det gäller information om hot som kan förmedlas från PTS ifrågasätter Hi3G Access AB om inte detta är något som Säkerhetspolisen ska förmedla enligt deras föreskrifter.

Vidare anser operatören att kraven på att nya hot ska analyseras ska begränsas så att sådana riskanalyser inte behöver göras vid alla förändringsarbeten.

Myndigheten för samhällsskydd och beredskap har gjort tolkningen att kraven på beaktande av ytterligare hot i riskanalysen utgör ett resultat av den nationella riskanalys som PTS har varit med att ta fram för antagonistiska risker kopplade till 5G. Myndigheten framför att man genom att räkna upp vissa hot riskerar att utelämna andra viktiga hot.

*PTS kommentarer:*

*PTS anser att sabotage mycket väl kan vara ett hot som måste hanteras i driftsäkerhetshänseende. När det gäller att den typen av hot redan kan omfattas av säkerhetskyddslagstiftningen anser PTS att så kan det mycket väl vara, men eftersom reglerna om driftsäkerhet delvis har ett annat mål och tillämpningsområde, så är det relevant att även riskanalyser kopplade till driftsäkerheten hanterar hotet sabotage. PTS ser inte att det är lämpligt att endast viss kritisk infrastruktur eller vissa förändringar ska omfattas av analys av hotet sabotage, däremot blir t.ex. konsekvenserna av sabotaget olika för olika t.ex. tillgångar, vilket medför att risken och de efterföljande skyddsåtgärderna beaktar skillnader i hur kritisk infrastruktur det rör. När det gäller förändringsarbeten är kravet på genomförande av riskanalys redan idag begränsat till sådana förändringar som kan orsaka störningar och avbrott av betydande omfattning.*

*Även när det gäller information som PTS kan förmedla om hot ser myndigheten att det kan vara en betydande skillnad mellan vad som är syftet att uppnå med säkerhetsskyddslagstiftningen jämfört med den rimliga nivån av driftsäkerhet som dessa föreskrifter ska säkerställa.*

*PTS arbete med att ta fram de aktuella förslagen till ändringar har inte någon koppling till det nämnda regeringsuppdraget om nationell riskanalys för 5G, utöver att PTS har kunnat använda sig av information som inhämtats inom ramen för det arbetet. PTS anser vidare att det är en bra ordning att uttryckligen nämna hot som måste riskanalyseras och att därtill lägga till alla andra "relevanta hot". De hot som uttryckligen nämns som måste analyseras är sådana som t.ex. incidentrapportering och PTS tillsyn och erfarenheter i övrigt har visat ett särskilt behov av att omfatta i riskanalys.*

## 4.3 Ytterligare tidpunkt för riskanalys

Hi3G Access AB ifrågasätter bl.a. hur man ska genomföra riskanalys av annans personal, samt vad en riskanalys inför upphandling ska kunna leda till för åtgärder, förutom att man inte använder sig av den tillgången/förbindelsen/uppdragstagaren.

Myndigheten för samhällsskydd och beredskap anser att bestämmelsen om riskanalys vid upphandling är otydlig såtillvida att det är oklart om det är risker med själva upphandlingen som avses.

Telenor Sverige AB uppger att det är en naturlig del av operatörens inköpsprocess att analysera säkerhet i samband med införskaffning av såväl utrustning som tjänster. Telenor Sverige AB kräver bl.a. ett gediget underlag och säkerhetsutfästelser från potentiella avtalspartners.

*PTS kommentarer:*

*Att t.ex. använda annans personal som uppdragstagare för olika uppdrag kopplade till driften av nät och tjänster innebär en uppenbar risk att tillhandahållaren inte har tillräcklig kontroll över sin verksamhet. I syfte att så långt det är möjligt reducera riskerna kopplade till annans personal är det enligt PTS bedömning nödvändigt att först genomföra en riskanalys kopplat till sådan användning. Samtliga relevanta hot för driftsäkerheten ska då beaktas, innefattande samtliga hot som räknas upp i 5 § föreskrifterna.*

*Det är upp till tillhandahållaren att efter genomförd analys säkerställa att rätt åtgärder vidtas. Det behöver inte vara att man inte använder sig av en viss utrustning eller uppdragstagare, utan kan innebära att man t.ex. begränsar åtkomster för vissa uppdragstagare till vissa tillgångar eller att man accepterar en lägre kvalitetsnivå eftersom man har en redundant lösning med en annan leverantör etc.*

*Det som ska analyseras i riskanalys, såväl inför upphandling som löpande, är risken för störningar och avbrott. Är det så att t.ex. väderrelaterade hot inte är relevant att analysera för t.ex. en uppdragstagare, så är riskvärdet noll för det aktuella hotet inför upphandlingen, varför inga skyddsåtgärder för att hantera väderhot behöver vidtas.*

## 4.4 Skyddsåtgärder som vidtas efter att PTS har förmedlat information om hot

Tele2 Sverige AB har framfört att man anser att paragrafen som innebär att skyddsåtgärder ska vidtas efter riskanalysen borde kunna slås ihop med nuvarande paragraf om vidtagande av skyddsåtgärder efter riskanalys.

Telenor Sverige AB framför bl.a. att man inte vill se en ordning där kravet på beaktande av information som förmedlas från PTS om hot kan användas för att kräva att operatörerna vidtar åtgärder som går utöver vad som är rimligt enligt driftsäkerhetsföreskrifterna.

ServaNet AB anser att det är ett retroaktivt krav att PTS kan informera om vissa hot som sen måste beaktas.

*PTS kommentar:*

*PTS håller med om att det egentligen inte hade behövts en helt egen paragraf om detta men har valt att göra så för att tydliggöra att det är en nyhet i reglerna. PTS tar dock med sig Tele2 Sverige ABs förslag till den kommande revideringen.*

*PTS kommer vid tillsyn beakta vilka åtgärder som är rimliga eller proportionerliga att kräva att en operatör vidtar med stöd av driftsäkerhetsreglerna.*

*Tillhandahållare ska kontinuerligt analysera riskerna i sin verksamhet utifrån aktuella hot, och därefter vidta lämpliga skyddsåtgärder. Att PTS ges en möjlighet att vidarebefordra information om hot är således bara ytterligare ett sätt för tillhandahållare att löpande erhålla information om relevanta hot.*

### 4.5 Tydliggörande avseende åtkomst och behörighet

Myndigheten för samhällsskydd och beredskap framför att man anser att dokumentationen över behörigheter bör sparas i minst fem år.

Telenor Sverige AB uppger att operatören inte gör någon skillnad mellan annan eller egen personal, men att det normalt inte är möjligt att på egen begäran få annans personal registerkontrollerade. Där är förfarandet istället att det initieras av den egna arbetsgivaren, men i tillämpliga fall sker det på Telenors Sverige ABs begäran.

Svenska stadsnätsföreningen anser att det är bra att endast behöriga har åtkomst till tillgångar men lyfter frågan om man med skrivningarna missar de kunder som finns till nätägaren, som i sin tur kan anlita någon.

*PTS kommentarer:*

*PTS håller med Myndigheten för samhällsskydd och beredskap om att det är en god idé att dokumentation om tilldelade behörigheter sparas. Det finns inte utrymme att närmare utreda frågan inom ramen för detta arbete, men PTS kan komma att beakta detta inom ramen för det kommande föreskriftsarbetet.*

*PTS håller även med Svenska stadsnätsföreningen om att det kan finnas osäkerheter vad som gäller för de som anlitar uppdragstagare i flera led. Enligt PTS bör nätägaren i dessa fall ställa krav på operatören att denne tillser att erforderliga behörigheter även finns för den som denne anlitar.*

# 5 Kommentarer på konsekvensutredningen

#### 5.1.1 Namngivande av enskild leverantör

Såväl Huawei Technologies Sweden AB som Tele2 Sverige AB har framfört synpunkter på att en enskild leverantör namnges i konsekvensutredningen.

*PTS kommentar:*

*PTS har, efter att konsekvensutredningen expedierats, varit i kontakt med Huawei Technonologies Sweden AB i syfte att diskutera varför PTS omnämner HCSEC och den granskningsrapport som finns publikt tillgänglig om företagets säkerhetsbrister. PTS har härvid framfört att anledningen till att detta nämns är för att det vid tidpunkten för författandet av konsekvensutredningen var den enda kända källan till information av detta slag som fanns att tillgå. Hade motsvarande rapport eller granskning funnits för övriga leverantörer hade PTS även hänvisat till dessa. PTS ser i detta hänseende inte att det skulle vara något negativt för företaget att man kan visa att man varit föremål för säkerhets-granskning.*

*Konsekvensutredningen utgör inte en rättskälla eller förarbete till kraven, utan är en redogörelse för motivering till krav och dess konsekvenser. Kraven i sig differentierar inte mellan olika aktörer utan det är riskanalysen som blir avgörande för val av leverantör.*

### 5.1.2 Redovisning av kostnader och konsekvenser

Telenor Sverige AB framför bl.a. att det inte är tydligt vilka förväntningar PTS har på t.ex. skyddsåtgärder när det rör sig om hantering av hot som inte är kända. Enligt operatören är det bra att skyddsåtgärderna ska stå i proportion till riskbedömningen, kostnaderna och verksamhetens art och omfattning, men uttrycker att det är oklart vad detta innebär i realiteten, och vad PTS förväntansbild är, när det gäller att hantera ovannämnda hot.

*PTS kommentar:*

*PTS har förståelse för att det hade varit tydligare och mer förutsägbart med redan angivna hot eller skyddsåtgärder att vidta. Men i och med att tekniken, hoten och samhället ständigt ändras och utvecklas blir den typen av kravställning lätt obsolet och utdaterad, vilket innebär att man istället får ställa krav på den här öppna nivån. Såsom Telenor Sverige AB också nämner så ska givetvis en proportionalitetsbedömning göras och PTS krav kan aldrig gå längre än att nyttan med kravet väger upp för t.ex. kostnaderna.*

### 5.1.3 Påverkan på konkurrens m.m.

Hi3G Access AB framför farhågor om att reglerna inte gäller för t.ex. avtal om upphandling som inträffat före 1 mars 2020, fastän upphandling för utbyggnad av 5G-nät redan påbörjats, vilket bl.a. kan få betydande påverkan på konkurrensen.

*PTS kommentarer:*

*När det gäller tillgångar och förbindelser som redan upphandlats före 1 mars 2020 så gäller ju redan att dessa löpande ska riskanalyseras i enlighet med befintliga krav. Det är samma analys och skyddsåtgärder som ska vidtas för såväl kommande som befintlig infrastruktur. Det som de nya reglerna tillför är att man redan inför upphandling ska börja genomföra riskanalys för utrustningen, dvs. ytterligare en tidpunkt för riskanalys.*

*Dock stämmer det att de uppdragstagare som redan anlitats före 1 mars 2020 inte per automatik kommer att behöva ha omfattats av en riskanalys inför upphandling, vilket PTS har bedömt få en godtagbar påverkan eftersom alternativet hade varit att inte införa ett krav på riskanalys inför upphandling av uppdragstagare.*

# 6 Avslutning

PTS gör en justering i sitt förslag till ändring av föreskrifter om krav på driftsäkerhet med anledning av remissvaren. Justeringen innebär att även uppdragstagares organisationsnummer ska dokumenteras.

I de fall där det i övrigt kan vara aktuellt med revidering mot bakgrund av inkomna synpunkter tar PTS med sig detta till det kommande arbetet med säkerhetsföreskrifter under 2020.

PTS vill slutligen tacka samtliga remissinstanser för inkomna synpunkter.

---

**Karin Lodin**, PTS avdelning för säker kommunikation

**Erica Nyström**, PTS rättsavdelning