Nasjonal sikkerhetsmyndighet

Vår saksbehandler	Vår dato	Vår referanse
Stab	2017-01-17	A03 - S:16/04122-16
	Deres dato	Deres referanse
	Antall vedlegg	Side
		1 av 25

Til
Forsvarsdepartementet
Postboks 8126 Dep
0032 OSLO

NOU 2016:19 Samhandling for sikkerhet - høringsuttalelse fra Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet (NSM) viser til departementets skriv av 17.10.2016 hvor NOU 2016:19 sendes på høring. Nedenfor følger NSMs uttalelse.

1 Oppsummering

De sentrale hovedpunktene i NSMs høringsuttalelse er:

- NSM støtter hovedinnretningen på det lovforslaget som er utarbeidet av Sikkerhetsutvalget, da dette kan bidra til en nødvendig heving av sikkerheten.
- Lovforslaget må imidlertid følges opp med en betydelig satsning på forebyggende sikkerhet i alle ledd. Uten en slik satsning vil kompleksiteten i forslaget kunne medføre en svekket sikkerhet sett opp mot dagens tilstand.
- Behovet for sektorovergripende reguleringer er mer omfattende enn hva utvalget foreslår. Det er en svakhet at implementering av NIS-direktivet i norsk rett og beskyttelse av den informasjon som i dag er regulert gjennom beskyttelsesinstruksen ikke er nærmere utredet. På disse områdene er det behov for en harmonisert tilnærming.
- Sikkerhetsmyndigheten og Tvisteorganet må gis en sterk lovforankret autoritet for å kunne styre og beslutte med bindende virkning overfor øvrige aktører. Dette er en nødvendig forutsetning for å sikre en enhetlig implementering av lovforslaget.

2 Innledning

NSM slutter seg til Sikkerhetsutvalgets beskrivelse av nåsituasjonen og dagens sikkerhetsutfordringer.

Utvalgets lovforslag representerer en utvidelse av gjeldende sikkerhetslovs saklige virkeområde. Dagens sikkerhetslov gir tverrsektorielle bestemmelser om beskyttelse av sikkerhetsgradert informasjon og skjermingsverdige objekter. Lovforslaget omfatter i tillegg informasjonssystemer som er av kritisk betydning for grunnleggende nasjonale funksjoner, men som ikke behandler sikkerhetsgradert informasjon, samt infrastruktur av kritisk betydning for grunnleggende nasjonale funksjoner.

Postadresse
Postboks 814
1306 SANDVIKA

Sivil telefon/telefaks
+47 67 86 40 00/+47 67 86 40 09
E-postadresse
post@nsm.stat.no

Militær telefon/telefaks
515 40 00/515 40 09
Internetadresse (URL)
www.nsm.stat.no

Utkast til ny sikkerhetslov inneholder mange gode elementer, og er langt bedre tilpasset dagens samfunnsutvikling enn eksisterende sikkerhetslov. NSM støtter i hovedsak innretningen på forslaget, og mener at dette vil legge til rette for en bedring av sikkerhetstilstanden og en god utvikling av denne. Behovet for sektorovergripende reguleringer er imidlertid mer omfattende enn utvalgets lovforslag. Det er en svakhet ved utredningen at implementering av NIS-direktivet i norsk rett og beskyttelse av den informasjon som i dag er regulert gjennom beskyttelsesinstruksen ikke er nærmere utredet. Beskyttelsestiltakene som følger av disse regimene vil i stor utstrekning være sammenfallende med de som foreslås regulert i ny lov om forebyggende nasjonal sikkerhet. Etter NSMs oppfatning er det uhensiktsmessig med flere parallelle regimer. Dette forsterkes ytterligere hvis forvaltningsansvaret fordeles ulikt. NSM mener at harmonisering på dette området er av stor betydning.

Forslaget forutsetter stor evne til å gjøre ulike komplekse sikkerhetsfaglige vurderinger. Både Sikkerhetsmyndigheten, sektormyndigheter og virksomheter stilles overfor dette for eksempel i arbeidet med å identifisere og utvelge virksomheter som skal være omfattet av loven, ved vurdering av forsvarlig sikkerhetsnivå, herunder gjennomføring av risiko og sårbarhetsanalyse, og ved gjennomføring av tilsyn. Lovforslaget er følgelig krevende å gjennomføre og vil fordre betydelig ressursinnsats, kompetanse og vilje til gjennomføring hos både Sikkerhetsmyndigheten, sektormyndigheter og virksomheter. For at en slik lov skal få ønsket effekt krever det, som utvalget påpeker, supplerende virkemidler. NSM mener en rekke tiltak bør iverksettes for å bidra til å gi loven ønsket effekt. Uten slike supplerende tiltak vil lovforslaget kunne resultere i en svekkelse av nasjonal sikkerhet.

Lovutkastet er formulert slik at det også tar hensyn til fremtidig samfunnsutvikling uten behov for større revisjoner. Enkelte bestemmelser og uttrykk er således rundt formulert. Dette kan skape rom for fortolkning og usikkerhet, og lovutkastet er således avhengig av en rekke presiseringer i forarbeider og i supplerende forskrifter. God innretning på forskriftene vil også kunne redusere belastningen på Tvisteorganet.

3 Generelle betraktninger

3.1 Formål

Formålsbestemmelsen er gitt en noe annen utforming enn i dagens sikkerhetslov. Det kan imidlertid stilles spørsmål ved om ordlyden reflekterer utvalgets intensjon om at loven skal gis et bredere nedslagsfelt. Formålsbestemmelsen fokuserer utelukkende på elementer som er en del av statssikkerheten, herunder vår nasjonale suverenitet, territorielle integritet og demokratiske styreform.

Lovens formål angis å være å motvirke uønskede hendelser mot disse interessene. Det kan også stilles spørsmål ved om begrepet «motvirke» er presist nok for lovens forebyggende innretning, eller om det heller burde vært benyttet begrepet «forebygge».

3.2 Begrepet grunnleggende nasjonale funksjoner

Lovforslagets virkeområde defineres ut fra begrepet «grunnleggende nasjonale funksjoner». NSM forstår det slik at begrepet «grunnleggende nasjonale funksjoner» vil konsumere

gjeldende lovs begreper som omfatter «rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser» og straffelovens, og utlendingslovens begrep «grunnleggende nasjonale interesser». Forslaget representerer derfor en utvidelse i forhold til dagens sikkerhetslov. NSM støtter en slik utvidelse.

Utvalget peker på at begrepet «andre vitale nasjonale sikkerhetsinteresser» i dagens sikkerhetslov aldri gjennomgikk den dynamiske utviklingen som lovgiver forutsatte da den ble vedtatt. NSM ser det derfor som positivt at det i det nye lovforslaget er inntatt en nærmere presisering av begrepets innhold gjennom fem tydelige kategorier. Erfaring med dagens lov har imidlertid vist at rettslige standarder i liten grad blir praktisert på en dynamisk måte. En proaktiv holdning for kontinuerlig å utvikle begrepets innhold vil derfor være helt nødvendig for å sikre en harmonisert tverrsektoriell utvikling.

3.3 Virkeområde

Utvalgets forslag til innretning av formål og virkeområde vil etter utvalgets egen vurdering sannsynligvis medføre at flere virksomheter blir underlagt loven.

Utvalget legger til grunn at de virksomheter som allerede i dag er omfattet av sikkerhetsloven, enten i kraft av å være forvaltningsorgan eller ved enkeltvedtak i medhold av gjeldende lov, også vil være omfattet av den nye loven. NSM slutter seg til disse betraktningene, men kan ikke se at dette er reflektert godt nok i lovforslaget. Lovforslaget legger til grunn at det også skal foretas individuelle vurderinger hva gjelder forvaltningsorganer. NSM mener at alle forvaltningsorganer i utgangspunktet bør være underlagt sikkerhetsloven. De fleste forvaltningsorganer vil kunne komme i en situasjon hvor de må behandle eller tilvirke sikkerhetsgradert informasjon. Dette vil særlig gjelde planlegning for og håndtering av krise og beredskapssituasjoner. Man må ikke komme i en situasjon hvor et forvaltningsorgan ved behov ikke har rettslig grunnlag for å behandle sikkerhetsgradert informasjon.

NSM mener på denne bakgrunn at den del av sikkerhetslovens nåværende virkeområdebestemmelse som automatisk legger forvaltningsorganer inn under loven bør videreføres. Utvalgets forslag om at det enkelte departement skal fatte vedtak om hvilke virksomheter som er av kritisk betydning for grunnleggende nasjonale funksjoner, og således være underlagt loven, bør derfor avgrenses til virksomheter som ikke er forvaltningsorganer. I de tilfeller hvor et forvaltningsorgan åpenbart ikke har en kritisk betydning for grunnleggende nasjonale funksjoner bør det heller åpnes for at det, som i dag, kan gjøres unntak fra lovens virkeområde. Det synes også lite formålstjenlig å skulle foreta slike vurderinger i forhold til forvaltningsorganer ut fra det premisset utvalget legger til grunn om at disse uansett vil være omfattet av den nye loven.

For å sikre at alle virksomheter, ut over forvaltningsorganer, som har behov for tilgang til sikkerhetsgradert informasjon på en enkel måte omfattes av loven, mener NSM at følgende bør vurderes inntatt som et nytt andre ledd i § 1-2.

Loven gjelder for alle virksomheter som vil, eller vil kunne, motta, tilvirke eller behandle sikkerhetsgradert informasjon.

Nærmere om hvilke virksomheter dette vil omfatte følger av merknad til § 2-1.

Hvis utvalgets forslag videreføres bør det, for å sikre kontinuitet for offentlige virksomheter som er underlagt dagens sikkerhetslov, gis en overgangsbestemmelse som sier at forvaltningsorganer vil være omfattet av loven inntil prosessen som beskrevet i § 2-1 er gjennomført og forvaltningsorganet gjennom denne har blitt vurdert og evt. blir besluttet unntatt fra loven. Hvis denne tilnærming velges må det også etableres en mekanisme som tydeliggjør hvor ansvaret ligger for å gjøre vurderinger knyttet til kommuner og fylkeskommuner.

3.4 Spesielt om sikkerhetsgradert informasjon

Hva angår sikkerhetsgradert informasjon er dette informasjon som har det samme beskyttelsesbehov uavhengig av i hvilken sektor eller virksomhet informasjonen håndteres. Dette fordi skadefølgene ikke bare rammer virksomheten, men bredere nasjonale interesser. Informasjonen kan også være mottatt fra internasjonale organisasjoner eller bilaterale samarbeidspartnere under forutsetning om beskyttelse etter visse minimumskrav. NSM mener derfor det er helt sentralt at det etableres en tydeligere tverrsektoriell forpliktelse til å beskytte sikkerhetsgradert informasjon knyttet opp mot nærmere definerte minimumskrav. I utvalgets forslag er dette kun reflektert i § 5-2 under kapittelet om informasjonssikkerhet. NSM vil påpeke viktigheten av at minimumskrav til beskyttelse av sikkerhetsgradert informasjon må kunne stilles innen alle relevante fagområder og ikke bare knyttet til informasjonssikkerhet. Dette må tydeliggjøres i lovforslaget. Videre bør Sikkerhetsmyndigheten kunne tillegges eneansvar for tilsyn med beskyttelse av sikkerhetsgradert informasjon.

3.5 Roller og ansvar

Lovforslaget tillegger departementene, sektortilsyn og andre sektormyndigheter, Sikkerhetsmyndigheten og tvisteorganet sentrale oppgaver.

3.5.1 Departementene

Departementenes rolle er i lovforslaget tydeliggjort og styrket. Departementene har betydelige oppgaver knytte til å etablere oversikt innen egen sektor, og fatte avgjørelse om hvilke virksomheter som skal underlegges loven. En god gjennomføring og oppfølging av dette ansvaret er helt sentralt for at loven skal kunne fungere etter sitt formål.

NSM støtter forslagets ansvarliggjøring av departementene, men ser at et system hvor departementet selv gjør vurderinger av hva som er av kritisk betydning for grunnleggende nasjonale funksjoner, åpner for en uensartet praksis mellom sektorene. NSM har erfart en uensartet praksis mellom departementene knyttet til de vurderinger som etter nåværende lov skal gjøres i forhold til hva som skal anses som skjermingsverdig objekt. Det er også NSMs erfaring at departementene i liten utstrekning etter dagens regelverk har fremmet forslag til Forsvarsdepartementet om underleggelse av private rettssubjekter. En mekanisme for bindende tvisteløsning ved uenighet knyttet til disse vurderingene er derfor av avgjørende betydning.

Videre mener NSM dette er et område der supplerende virkemidler med fordel kan benyttes for å bidra til ønsket effekt. Utvikling av et metodisk grunnlag for kartlegging, samt tilhørende verktøy og veiledning bør igangsettes slik at dette er klart før lovens ikrafttredelse.

3.5.2 Sikkerhetsmyndigheten

Lovforslaget forutsetter en sterk Sikkerhetsmyndighet. NSM mener at oppgavebeskrivelsen i § 2-2 ikke i tilstrekkelig grad legger til rette for at sikkerhetsmyndigheten skal kunne drive aktiv styring av arbeidet med forebyggende sikkerhet. Videre er rollen som fagmyndighet og internasjonalt kontaktpunkt for utydelig beskrevet. En proaktiv faglig utvikling må være en sentral oppgave for Sikkerhetsmyndigheten. I en internasjonal kontekst er Norge forpliktet til å etablere ulike sikkerhetsfunksjoner som kontaktpunkt mot andre land og internasjonale organisasjoner. Dette omfatter blant annet rollene som National Security Authority, National Distribution Authority, National Communication Security Authority og National Tempest Authority. NSM forutsetter at disse funksjonene som i dag vil tilligge Sikkerhetsmyndigheten. Disse forpliktelsene bør på overordnet nivå reflekteres i lovteksten.

For å styrke sikkerhetsmyndighetens rolle mener NSM videre at følgende oppgaver fra dagens lov må videreføres.

a. innhente og vurdere informasjon av betydning for gjennomføringen av forebyggende sikkerhetstjeneste.

Denne oppgaven er særdeles viktig for at sikkerhetsmyndigheten skal ha nødvendige hjemmelsgrunnlag for innhenting av informasjon som er grunnlag for myndighetens aktiviteter.

I tillegg bør følgende bestemmelser videreføres:

b. utøvende organ i forhold til andre land og internasjonale organisasjoner
c. søke internasjonalt samarbeid, herunder med andre lands og organisasjoners tilsvarende tjenester, når dette tjener norske interesser,
d. bidra til at sikkerhetstiltak utvikles, herunder iverksette forskning og utvikling på områder av betydning for forebyggende sikkerhetstjeneste,

Vi vil påpeke at også visse andre fagtunge funksjoner må utøves sentralt og ikke kan ivaretas av sektormyndighetene. Et eksempel på dette er myndighetsgodkjenning av krypto. NSM legger til grunn at den rollen som NSM har på kryptoområdet i dag blir videreført og nærmere regulert i forskrift. Det bør også vurderes om dette skal defineres som en oppgave for Sikkerhetsmyndigheten i § 2-2.

Utvalgets beskrivelse av sikkerhetsmyndighetsfunksjonen synes å legge opp til utstrakt rådgivning fra Sikkerhetsmyndigheten til enkeltvirksomheter. Dette er etter NSMs oppfatning en lite kosteffektiv tilnærming. NSM mener at en «en-til-mange» tilnærming er mer hensiktsmessig når det gjelder rådgivning, der dette er mulig. I den grad det er ønskelig at NSM skal bedrive rådgivning overfor enkeltvirksomheter må det fremkomme at NSM selv kan prioritere hvem som skal motta slik rådgivning, basert på sin kunnskap om risiko. En

forventning om utstrakt «en-til-en» rådgivning fra NSM vil også fordre en betydelig styrkning av organisasjonen. Dette bør reflekteres i videre lovarbeid.

3.5.3 Tvisteorganet

Lovforslaget etablerer et tvisteorgan som skal ta standpunkt til uenighet knyttet til praktisering av enkelte av lovforslagets bestemmelser.

Basert på erfaringer med gjeldende sikkerhetslov ser NSM det som hensiktsmessig at det etableres en mekanisme for å avgjøre saker hvor det er uenighet. En suksessfaktor for forslaget er at Tvisteorganet gis nødvendig besluttende myndighet. Med det handlingsrom lovforslaget gir, både til departementene, sektormyndighetene og virksomhetene vil det være av avgjørende betydning for å sikre en harmonisert praksis at de avgjørelser tvisteorganet fatter er bindende for så vel forvaltningen som for private rettssubjekter.

3.6 Begreper

Utvalgets lovforslag inneholder ikke en egen bestemmelse om definisjoner. Av pedagogiske hensyn bør det vurderes om det skal inntas en bestemmelse som definerer de mest sentrale begreper i lovforslaget. Lovforslaget benytter en del begreper som vil være rettslige standarder, som for eksempel grunnleggende nasjonale funksjoner og forsvarlig sikkerhetsnivå. Dette er begreper hvis innhold vil kunne endres i takt med samfunnsutviklingen. NSM legger til grunn at Sikkerhetsmyndigheten i sine veiledninger autoritativt må kunne fortolke disse begrepene.

3.7 Tilsyn

Lovforslaget legger til grunn at det primært er sektortilsyn (der slike er etablert) som skal følge opp implementeringen av lovens krav.

Hensynet til bransjespesifikk kunnskap og hensynet til å unngå dupliserende tilsyn er anført som bakgrunn for forslaget til en delt tilsynsmodell. NSM er enig i at dette er viktige hensyn. Kunnskap om den enkelte sektors særegenheter må imidlertid balanseres mot andre viktige hensyn, herunder hensynet til en effektiv utnyttelse av tilsynsressursene og hensynet til en helhetlig og tverrsektoriell tilnærming ivaretatt gjennom et samlet og robust fagmiljø innen forebyggende sikkerhet. Vi stiller derfor spørsmål ved om den forslåtte ordningen med oppbygging av dupliserende kompetanse er den mest hensiktsmessige og effektive ressursutnyttelsen, fremfor å styrke Sikkerhetsmyndigheten.

For en forsvarlig implementering av forslaget er det påkrevd at sektortilsyn har den nødvendige kompetanse på forebyggende sikkerhet. Dette er kompetanse som mange sektortilsyn ikke har i dag. En forutsetning for en slik tilsynsmodell er derfor at Sikkerhetsmyndigheten, i tillegg til å utarbeide kriterier for tilsyn og forestå opplæring, også må kunne ha innflytelse med hensyn til hvilke sektortilsyn som vurderes som faglig kvalifisert, herunder stille krav til sektortilsynenes kompetanse, og føre tilsyn.

For å unngå en ressurskrevende dublering av kompetansemiljøer vil det etter NSMs oppfatning bare være tilsyn av en viss størrelse, for eksempel NKOM, som vil kunne ha forutsetninger for å utøve et faglig forsvarlig tilsyn etter loven. Det må derfor vurderes konkret

i hvilke sektorer det ligger til rette for at sektortilsyn ivaretar oppgaver etter loven. Der forutsetningene ikke er til stede må departementene utvise varsomhet med å tillegge sektormyndigheter kompetanse etter loven.

Det bør også vurderes nærmere om tilsyn innen fagområder hvor hensynet til sektorspesifikk kunnskap i mindre grad gjør seg gjeldende, bør forbeholdes Sikkerhetsmyndigheten. Det bør derfor etableres en forskriftshjemmel til å fastsette at Sikkerhetsmyndigheten kan gis enekompetanse for tilsyn på visse fagområder. Dette vil typisk være knyttet til beskyttelse av sikkerhetsgradert informasjon, herunder håndtering av krypto og personellsikkerhet.

Det er videre en nær sammenheng mellom funn fra tilsyn og Sikkerhetsmyndighetens oversikt over det nasjonale sikkerhetsbildet og andre sektorovergripende oppgaver Sikkerhetsmyndigheten er tillagt. NSM ser at den foreslåtte ordningen med delt tilsynsansvar kan innebære en svekkelse av Sikkerhetsmyndighetens mulighet til å ivareta rollen som sektorovergripende fagmyndighet som forutsatt etter § 2-2. NSM foreslår derfor justeringer av ordlyden i flere av bestemmelsene i tilsynskapitlet for å kompensere for de ulemper en delt tilsynsmodell kan innebære.

3.8 Behandling av personopplysninger

Behandling av personopplysninger er gitt en fragmentert regulering i lovforslaget. Enkelte bestemmelser som §§ 2-4, 3-5 og 6-4 etablerer uttrykkelige hjemler for på avgrensede områder og til avgrensede formål å kunne behandle personopplysninger. Av andre bestemmelser følger adgangen til å behandle personopplysninger mer implisitt. Dette gjelder for eksempel lovforslagets bestemmelser om sikkerhetsklarering og autorisasjon, samt kommunikasjon- og innholdskontroll av kommunikasjonssystemer og inntrengningstesting.

NSM vil bemerke at personopplysninger også må behandles i andre tilfeller som ledd i den forebyggende sikkerhetstjeneste. Dette gjelder i særdeleshet aktivitet knyttet til håndtering, og herunder varsling, av sikkerhetstruende virksomhet og andre uønskede hendelser. NSM anbefaler på dette grunnlag at det vurderes å innta en samlet bestemmelse som gir en generell hjemmel for behandling av personopplysninger der dette er nødvendig for å ivareta de plikter som følger av loven. Alternativt må det foretas en gjennomgang med tanke på å etablere tilstrekkelige særhjemler på alle områder hvor det innen forebyggende sikkerhetstjeneste er behov for å behandle personopplysninger.

4 NSMs kommentarer til de enkelte bestemmelsene

Til *§ 1-1 Lovens formål*

Formålsbestemmelsen slik den er formulert i forslaget er etter NSMs mening en hensiktsmessig tilnærming, som forhåpentligvis vil bidra til en helhetlig tilnærming til nasjonal sikkerhet som omfatter både det tradisjonelle statssikkerhetsperspektivet, men også omfatter deler av samfunnssikkerheten for øvrig. NSM mener imidlertid at ordlyden i bestemmelsen kan justeres noe for å tydeliggjøre begge perspektivene. Dersom man erstatter «ved å» med «og å» vil begge perspektivene omfattes av selve formålsbestemmelsen.

Alternativt kan følgende ordlyd i formålsbestemmelsen vurderes:

Loven skal bidra til å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og verne sentrale samfunnsinstitusjoner og vår felles sikkerhet *ved å forebygge tilsiktede hendelser som kan skade grunnleggende nasjonale funksjoner.*

Loven skal sikre at tiltak som iverksettes for å ivareta lovens formål, gjennomføres på en måte som er forenlig med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.

NSM ser ikke behovet for å presisere i lovtekst at tilsiktede hendelser som kan skade grunnleggende nasjonale funksjoner må omtales som «uønskede», da dette er dekke inn under kravet om skadefølger for grunnleggende nasjonale funksjoner. NSM mener at begrepet skaper et unødig komplisert språk.

Til *§ 1-2 Lovens virkeområde*
I første ledd bokstav c refereres det til forholdet til andre stater. Bestemmelsen bør utvides også til å omfatte forholdet til internasjonale organisasjoner, dette kan eksempelvis være NATO, EU, European Space Agency mv.

Begrepet virksomhet er ikke definert i lovforslaget. Basert på utvalgets spesielle merknader legger NSM til grunn at forslaget vil representere en videreføring av begrepet slik at det også omfatter de rettssubjekter som i dag er angitt i § 2 tredje ledd.

Til *§ 2-1 Departementenes ansvar og myndighet etter loven*
Virksomheter som mottar, behandler eller tilvirker sikkerhetsgradert informasjon må være omfattet av loven, jf. NSMs forslag til endringer i § 1-2.

NSMs forslag er at departementene bør ha ansvar for å treffe vedtak og holde oversikt over hvilke virksomheter dette vil gjelde. Det bør i så fall tilføyes et nytt første ledd bokstav d som lyder:

treffe enkeltvedtak om at virksomheter har behov for å motta, behandle eller tilvirke sikkerhetsgradert informasjon jf. § 1-2, slik at loven gjelder for dem.

Bestemmelsens andre til fjerde ledd må endres tilsvarende.

Til *§ 2-2 Sikkerhetsmyndigheten*
Det vises til NSMs generelle merknader.

Til *§ 2-3 Informasjon om trusselvurderinger og risikohåndtering*
NSM mener at denne bestemmelsen er viktig for å sette virksomhetene i stand til å gjøre gode risikovurderinger og implementere nødvendige sikkerhetstiltak. Bestemmelsen fordrer imidlertid at eiere av trusselvurderinger og annen sikkerhetsinformasjon har formell adgang og vilje til å produsere og dele slik informasjon.

NSM vil herunder bemerke at det er et generelt behov for å styrke deling av sikkerhetsrelevant informasjon mellom alle ledd innenfor det forebyggende sikkerhetsarbeidet. Et alternativ for denne bestemmelsen vil være å gjøre den mer generell og flytte den til kapittel 4. Overskriften bør da endres til *«Deling av sikkerhetsinformasjon»* og

det bør tilføres et nytt ledd som gir den enkelte virksomhet en plikt til å dele sikkerhetsinformasjon som man må forstå kan være av betydning for andre virksomheter.

Til *§ 2-4 Nasjonal responsfunksjon for alvorlige dataangrep*
Av ordlyden i bestemmelsens første ledd følger at *«Kongen utpeker en nasjonal responsfunksjon for alvorlige dataangrep mot skjermingsverdig infrastruktur og et nasjonalt varslingssystem for digital infrastruktur.»*

For å harmonere dette med lovforslagets virkeområde bør bestemmelsen endres til:

Kongen utpeker en nasjonal responsfunksjon for dataangrep mot grunnleggende nasjonale funksjoner og et nasjonalt varslingssystem for digital infrastruktur.

Til *§ 2-5 Vedtaksmyndighet for Kongen i statsråd*
NSM mener overskriften ikke i tilstrekkelig grad reflekterer det materielle innholdet i bestemmelsen, og foreslår at denne endres slik at den blir mer dekkende.

Til *§§ 2-6 Klage og tvisteløsning, og 2-7 Tvisteorgan for forebyggende nasjonal sikkerhet*
Det vises til de generelle merknadene i punkt 3.5.3 om tvisteorganet.

Til *§ 3-1 Tilsyn med virksomheter*
Lovforslaget foreslår en delt tilsynsmodell. Dette vil innebære at det er sikkerhetsloven med forskrifter som vil være hjemmelsgrunnlaget også for sektortilsynenes tilsynsvirksomhet.

I andre ledd foreslås det at ansvarlig departement kan bestemme at tilsynsansvaret skal legges til myndigheter som «har tilsynsfunksjoner som omfatter beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur». Oppregningen er alternativ, hvilket vil innebære at dersom et tilsynsorgan har tilsynsfunksjoner innen ett at disse alternativene, vil man kunne få et utvidet ansvar for å dekke hele bredden dersom ansvarlig departement beslutter det. Dette vil omfatte et bredt spekter av fagområder, herunder personellsikkerhet, IKT-sikkerhet, kryptosikkerhet og sikkerhetsgraderte anskaffelser. Det kan neppe forventes at det enkelte sektortilsyn besitter kompetanse innen hele spekteret av fagområder som omfattes av sikkerhetsloven. For å sikre at tilsynsmyndighet legges til et kompetent organ må sektortilsynene tilfredsstille Sikkerhetsmyndighetens krav til kompetanse. Før departementene fatter beslutning om hvilke sektortilsyn som skal føre tilsyn etter loven, må Sikkerhetsmyndigheten konsulteres.

NSM stiller også spørsmål ved om utvalgets forslag vil være den mest hensiktsmessige bruken av ressurser for Sikkerhetsmyndigheten og sektortilsynene totalt sett. For sektortilsynene som blir utpekt vil det innebære at man trolig må ansette ytterligere personell som har riktig kompetanse for å dekke fagområder utover de fagområder tilsynsmyndigheten ellers forvalter. Det vil medgå vesentlig med tid til å sette seg inn i et nytt regelverk, som i mange tilfeller kun sjelden vil komme til anvendelse. Sektortilsynene kan også risikere å måtte sette seg inn i og anvende en annen metodikk enn den man vanligvis benytter. Det vil kunne medføre en fragmentering av kompetansen, og at man innen statlig sektor vil måtte konkurrere om de samme ressursene, som det for enkelte fagområder er knapphet på. I denne sammenheng vises det til den nylig vedtatte endringen i sikkerhetsloven knyttet til

sentralisering av klareringsmyndighetene. Hensynet til å kunne bygge og vedlikeholde et kompetent og robust fagmiljø var ett av hovedargumentene bak denne lovendringen.

Enkelte fagområder fordrer en særlig kompetanse som det ikke er hensiktsmessig at flere tilsynsorganer besitter. Det bør derfor kunne fastsettes i forskrift at Sikkerhetsmyndigheten skal ha enekompetanse for gjennomføring av tilsyn innen enkelte fagområder, som for eksempel administrativ kryptosikkerhet, tilsyn med etterlevelse av ATOMAL forskriften og tilsyn med klareringsmyndighetene.

Der Sikkerhetsmyndigheten er godkjenningsansvarlig, f eks for et IKT-system, må kompetansen til å føre tilsyn også tilligge Sikkerhetsmyndigheten.

Etter lovforslaget er det uklart hvem som har tilsynskompetanse overfor systemer, infrastruktur og prosesser som går på tvers av sektorer. NSM forutsetter at dette er Sikkerhetsmyndighetens ansvar. Dette bør tydeliggjøres i lovforslaget.

Etter bestemmelsen fjerde ledd skal Sikkerhetsmyndigheten føre tilsyn med sektormyndigheter som er tillagt et tilsynsansvar etter loven. NSM vil måtte utvikle en ny metodikk for denne type tilsyn. Som ledd i et slikt tilsyn må Sikkerhetsmyndigheten ha anledning til også å føre tilsyn med enkeltvirksomheter i sektorene på stikkprøvebasis. Dette for å kunne vurdere kvaliteten på sektortilsynenes arbeid. En slik tilsynsrett bør lovfestes.

Til *§ 3-2 Sikkerhetsmyndighetens samarbeid med sektormyndigheter*
NSM er enige i at det bør tilstrebes at den totale belastningen for tilsynsobjektene ikke blir høyere enn nødvendig, som foreslått i bestemmelsens *andre ledd.* Vi slutter oss derfor til en koordineringsplikt for tilsyn generelt.

Til femte ledd vil NSM bemerke at Sikkerhetsmyndigheten må gis en avgjørende innflytelse på utvelgelse av tilsynsobjekter innen de ulike sektorer. Dette er nødvendig for å sikre helhetlig og sektorovergripende tilnærming til utvelgelsen av tilsynsobjekter. Dette vil også være avgjørende for NSMs evne til å holde et godt bilde over den nasjonale sikkerhetstilstanden. Det bør derfor synliggjøres i dette leddet at Sikkerhetsmyndigheten også skal medvirke ved utvelgelse av tilsynsobjekter.

I henhold til bestemmelsens sjette ledd kan sektormyndighetene anmode Sikkerhetsmyndigheten om bistand til gjennomføring av tilsyn. NSM legger til grunn at man ikke har noen ubetinget plikt til å etterkomme slike anmodninger, og at Sikkerhetsmyndigheten må kunne vurdere disse basert på en risikovurdering og ut fra de til enhver tid tilgjengelige ressurser.

Etter samme ledd er sektortilsynene rapporteringspliktige til Sikkerhetsmyndigheten om hovedfunn fra sine tilsyn. Dette er for snevert for at Sikkerhetsmyndigheten skal kunne ivareta sitt ansvar som tilsynsmyndighet overfor sektormyndighetene, jf. også § 3-6 tredje ledd. Skal Sikkerhetsmyndigheten ha et situasjonsbilde som gjør at denne siste bestemmelsen kan implementeres etter sin intensjon, må Sikkerhetsmyndigheten få gjenpart av alle tilsynsrapporter.

Til *§ 3-3 Generelle prinsipper for tilsyn*

I lovforslagets første ledd fastsettes det at tilsynet skal planlegges og gjennomføres slik at i minst mulig grad virker forstyrrende på tilsynsobjektets daglige drift. NSM slutter seg til denne tilnærmingen, men legger til grunn at bestemmelsen ikke kan benyttes av en virksomhet for å nekte tilsyn gjennomført eller for langvarig utsettelse. En slik presisering vil etter NSMs syn kunne ivaretas gjennom merknad til bestemmelsen i forarbeidene.

Det foreslås i bestemmelsens *andre ledd* at «Opplysninger som tilsynsmyndigheten innhenter som ledd i tilsynsvirksomheten skal bare nyttes i direkte forbindelse med tilsynet». Formuleringen er etter NSMs syn for snever. Det må være mulig for tilsynsmyndigheten (sikkerhetsmyndighet eller sektormyndighet) å samle og analysere tilsynserfaringer til bruk i risikovurderinger, for å forbedre sikkerhetstiltak og sikkerhetsarbeid, herunder videreutvikling av tilsynsvirksomheten, revurdering av gitte sikkerhetsmessige godkjenninger av systemer, samt forbedring av rådgivningsarbeidet. Dersom bestemmelsen blir vedtatt med den foreslåtte ordlyden frykter NSM at dette vil svekke både Sikkerhetsmyndighetens mulighet til å ivareta oppgavene i henhold til § 2-2, samt sektormyndighetenes mulighet for å forbedre sikkerheten i egen sektor.

Vi stiller for øvrig spørsmål ved om § 3-3 etter sitt innhold mer naturlig hører hjemme på forskrifts nivå.

Til *§ 3-4 Stedlig tilsyn*

NSM er positive til at tilsynsmyndighetens tilgangsrett presiseres. Vi foreslår imidlertid eksplisitt også å tilføye tilgang til å gjennomføre samtaler med virksomhetens personell. Eksempler på slikt personell er ledere, sikkerhetspersonell og øvrig relevante medarbeidere. I enkelte tilfeller har det vært en utfordring å få tilgang til relevant personell, noe som har medført at kvaliteten på den informasjon man har fått tilgang til har blitt redusert, og at utbyttet av tilsynet har blitt mindre enn ønskelig.

Det presiseres i bestemmelsens andre ledd andre punktum at forvaltningsloven § 15 gjelder tilsvarende. Henvisningen til denne bestemmelsen synes lite treffende med tanke på hvordan denne type tilsyn gjennomføres. I anerkjente revisjonsstandarder er det nedfelt en rekke prinsipper for god revisjonsskikk. I tillegg vil alltid prinsippene for god forvaltningsskikk ligge til grunn. Det bør derfor vurderes om henvisningen til forvaltningsloven § 15 er nødvendig. Etter NSMs oppfatning bør det for øvrig vurderes om andre ledd i sin helhet kan utgå.

Til *§ 3-5 Tilsynsmyndighetens behandling av personopplysninger*

NSM støtter at det etableres en hjemmel for behandling av personopplysninger i forbindelse med gjennomføring av tilsyn. Vi viser for øvrig til generelle merknader om behovet for en bredere hjemmel til å behandle personopplysninger innen forebyggende sikkerhetstjeneste.

NSM stiller spørsmål ved hensiktsmessigheten av bestemmelsens tredje ledd. En slik bestemmelse vil vesentlig vanskeliggjøre tilsynsvirksomhet. Tilsyn forberedes i dag i NSMs lokaler og som ledd i dette innhentes informasjon fra virksomheten. Tilsyn kan også gjennomføres papirbasert gjennom for eksempel innhenting av en virksomhets saksdokumenter. Innen enkelte fagområder benyttes også virksomhetsovergripende IKT-

systemer. Et effektivt tilsyn fordrer at tilsynsmyndigheten kan gå direkte inn og hente informasjon ut fra disse. NSM vil på denne bakgrunn foreslå at tredje ledd strykes.

Til *§ 3-6 Pålegg*

Utvalgets forslag synes å bygge på et premiss om at tilsyn munner ut i pålegg om gjennomføring av konkrete sikkerhetstiltak. NSMs tilsynsmetodikk har imidlertid en annen tilnærming. Dersom det konstateres manglende samsvar med regelverket, gis det avvik fra de aktuelle bestemmelsene og pålegg om å korrigere avvikene, uten at det er konkretisert hvordan avvikene skal korrigeres. Både ut fra en erkjennelse om at det som regel er den enkelte virksomhet som er nærmest til å finne de de beste løsningene for sin virksomhet, og også for å sikre virksomhetens eierskap til løsningen og prosessene med å gjennomføre tiltakene, vil det da være opp til virksomheten å korrigere slik at forholdene bringes i samsvar med kravene. Med denne metodiske tilnærmingen synes kriteriene som stilles i første ledd mindre treffende.

Det vil være rent unntaksvis at det pålegges gjennomført konkrete tiltak. For de tilfeller tilsynsmyndigheten ser behov for å pålegge konkrete tiltak vil kravet om at det er «utvilsomt at tiltaket er nødvendig» være for strengt. Det bør være tilstrekkelig at tiltaket fremstår som «nødvendig». Første ledd bør på denne bakgrunn reformuleres.

I andre ledd bør det presiseres at Sikkerhetsmyndighetenes påleggskompetanse også gjelder i forhold til departementene og andre virksomheter som Sikkerhetsmyndigheten har tilsynskompetanse overfor.

Etter tredje ledd kan Sikkerhetsmyndigheten gi pålegg til sektormyndighetene. Dette begrunnes i at Sikkerhetsmyndigheten skal *«kunne gripe inn overfor en sektormyndighet dersom det skulle vise seg at sikkerhetsnivået i den aktuelle samfunnssektoren utvikler seg på en utilfredsstillende måte».* Imidlertid kan det være vanskelig for Sikkerhetsmyndigheten å få kunnskap om dette, og derfor vite når det er behov for å gripe inn. Det vises i denne sammenheng til merknader til § 3-2.

Til *§ 4-1 Plikt til å gjennomføre sikkerhetstiltak*

NSM støtter tilnærmingen om at forebyggende sikkerhetstiltak skal utformes med bakgrunn i en risikoanalyse. I lovforslaget benyttes begrepet «*Risiko- og sårbarhetsanalyse».* Dette er etter NSMs oppfatning ikke en presis betegnelse. «*Risiko»* er et hypernym (overbegrep) som omfatter sårbarhet i tillegg til trussel og verdi, jf. NS 5832 og *trefaktormodellen* risikoanalyse. Det korrekte begrepet vil på denne bakgrunn være Risikoanalyse. Dette bør benyttes konsekvent i lovteksten.

Virksomheten bør som ledd i dette også ha en plikt til å gjøre vurderinger rundt hvilke trussel aktører og senarioer som er aktuelle, og som skal være dimensjonerende for de tiltak som iverksettes.

Lovforslaget legger i stor utstrekning opp til at sikkerhetstiltakene skal gjennomføres i henhold til den enkelte virksomhets risikoanalyse. Sikkerhetstiltakene skal være *forsvarlige*. Forsvarlighetsvurderingen skal gjøres av virksomheten selv, men under forutsetning av bistand fra sektormyndigheten og Sikkerhetsmyndigheten samt tilgang på tilstrekkelig

informasjon om trusselbildet. Ved denne tilnærmingen gis virksomhetene en avgjørende innflytelse på hvilke sikkerhetstiltak som skal implementeres. Kostnader forbundet med tiltakene skal vurderes av den enkelte virksomhet. NSM tror at en så høy grad av skjønnsmessigutøvelse i den enkelte virksomhet kan medføre en ulik tilnærming til forsvarlighetskravet.

Vi legger derfor til grunn at forsvarlighetskravet vil være gjenstand for tilsyn og at Sikkerhetsmyndigheten og sektormyndighetene vil ha et fortolkningsansvar og dermed en bestemmende innflytelse på forståelsen av begrepet. Dette, sammen med god informasjon om trusselvurdering og annen sikkerhetsinformasjon, vil være nødvendig for å oppnå en enhetlig og harmonisert praksis.

NSM mener at § 4-1 også bør gis en overordnet beskrivelse som tilrettelegger for tiltak som sikrer beskyttelse i dybden. Vi mener derfor at dagens systematikk knyttet til objektsikkerhet bør etableres som et generelt prinsipp ved at første ledd bokstav a endres til;

gjennom en kombinasjon av barrierer, deteksjon, reaksjon og evne til gjenoppretting bidra til å hindre (…).

Til *§ 4-2 Sikkerhetsstyring*
NSM støtter forslaget. Sikkerhetsstyring er sentralt for det systematiske arbeidet med sikkerhet i virksomhetene, og vi anser det derfor som viktig at det gis en slik bestemmelse i loven.

Til *§ 4-3 Risiko- og sårbarhetsanalyse*
Overskriften i bestemmelsen bør endres til «Risikoanalyse», under henvisning til vår merknad til § 4-1.

Det er sentralt at virksomhetene har samme metodiske tilnærming til de risikoanalyser som skal gjøres. NSM legger derfor til grunn at man i forskrift vil gi nærmere bestemmelser om hvordan disse analysene skal gjennomføres og hvem som skal etablere det metodiske grunnlaget.

Til bestemmelsens første ledd vil vi bemerke at virksomheten også må kartlegge hvilke sikkerhetskrav den er bundet av gjennom regelverk, godkjenninger mm. Dette bør synliggjøres i bestemmelsen.

Til *§ 4-4 Krav til dokumentasjon*
Bestemmelsen beskriver krav til dokumentasjon som skal foreligge hos virksomhetene. Det er et viktig krav og det er positivt at dette fremkommer klart.

Til *§ 4-5 Øvelser*
Øvelser er viktige for å gi ansatte kunnskaper og ferdigheter innen håndtering av sikkerhetshendelser. Det er også viktig å gjennomføre øvelser for å avdekke eventuelle feil/mangler ved relevant planverk som virksomheten har utviklet. NSM er derfor positive til forslaget, og legger til grunn at kravet til «regelmessige øvelser» eventuelt kan konkretiseres i forskrift.

Til *§ 4-6 Varsling*
Til bestemmelsens tredje ledd bemerkes at det i enkelte tilfeller kan være uklart hvilket departement som er ansvarlig. Dette gjelder for eksempel ved varsler mottatt fra kommunale organer, eller varsler som dreier seg om privat virksomhet uten en klar departementstilknytning, for eksempel datahaller. NSM legger til grunn at varsel i disse tilfellene skal sendes til Justis- og beredskapsdepartementet i kraft av departementets samordningsrolle på sivil side. Det bør imidlertid vurderes om dette skal tydeliggjøres i lovteksten eller eventuelt i forskrift.

I dagens forskrift om sikkerhetsadministrasjon § 5-7 følger at virksomheten ved sikkerhetstruende hendelser skal vurdere å orientere eller avgi anmeldelse til politiet/PST. NSM ser et behov for at denne bestemmelsen videreføres. Det bør vurderes nærmere om dette skal skje på lovs nivå eller videreføres i forskrift som i dag.

Til *§ 4-7 Behandling av personopplysninger*
NSM har ingen merknader til bestemmelsen, men viser til punkt 3.8 ovenfor.

Til Kapittel 5. Informasjonssikkerhet
Etter NSMs oppfatning gir kapittelets overskrift et noe misvisende inntrykk. Kapittelet omhandler etter sitt innhold kun bestemmelser om gradering og beskyttelse av sikkerhetsgradert informasjon. Kapittelets overskrift bør derfor endres til «Beskyttelse av sikkerhetsgradert informasjon». På den annen side fremstår ikke kapitelet som uttømmende i forhold til de krav som må stilles til beskyttelse av sikkerhetsgradert informasjon, og må således sees i sammenheng med andre kapitler i lovforslaget. Om utvalgets forslag til lovstruktur er hensiktsmessig på dette punkt bør derfor vurderes nærmere.

Til *§ 5-1 Sikkerhetsgradert informasjon*
Det vil være virksomheter som er omfattet av loven som har kompetanse til å utstede og tilvirke sikkerhetsgradert informasjon. Det bør tydeliggjøres at det er virksomheten som er pliktsubjekt. Bestemmelsen bør derfor lyde:

Virksomhet som utsteder eller på annen måte (…)

Begrepet grunnleggende nasjonale funksjoner er vurderingskriteriet i forhold til sikkerhetsgradering. NSM vil påpeke viktigheten av at begrep blir operasjonalisert på en god måte, eksempelvis gjennom retningslinjer. Dette kan best skje i den enkelte sektor, men Sikkerhetsmyndigheten som sektorovergripende organ må trekkes inn i arbeidet for å legge til rette for en god tverrsektoriell nivellering. Det bør vurderes nærmere bestemmelser om dette i forskrifts form.

Til *§ 5-2 Beskyttelse av sikkerhetsgradert informasjon*
NSM slutter seg til de overordnede prinsipper som defineres for beskyttelse av sikkerhetsgradert informasjon.

Sikkerhetsgradert informasjon må beskyttes i henhold til etablerte minstestandarder som gjelder uavhengig av hvilken sektor informasjonen behandles. Dette er nødvendig for å oppnå en helhetlig beskyttelse. For å unngå parallelle regelsett, og samtidig ivareta våre forpliktelser overfor andre stater og internasjonale organisasjoner som NATO, er disse

minstestandardene nødvendige. NSM slutter seg derfor til at det i forskrift kan gis minstekrav for beskyttelse av sikkerhetsgradert informasjon. Vi legger til grunn at minstestandardene som minimum vil reflektere de krav som følger av NATO Security Policy, og som også de fleste andre europeiske land legger til grunn for sine nasjonale regler.

De minstekrav som hjemles i § 5-2, andre ledd må omfatte alle relevante fagområder for beskyttelse av sikkerhetsgradert informasjon. Dette omfatter også krav til informasjonssystemer som behandler slik informasjon (herunder bruk av krypto) jf. kapittel 6, til personell som skal ha tilgang til slik informasjon jf. kapittel 8 og til leverandører i forbindelse med sikkerhetsgraderte anskaffelser jf. kapittel 9. Det må også kunne stilles minstekrav til virksomheters sikkerhetsorganisasjon og sikkerhetsstyring jf. kapittel 4.

På denne bakgrunn bør det vurderes om denne forskriftshjemmelen mer naturlig hører hjemme i kapittel 4.

Til *§ 5-4 Tekniske sikkerhetsundersøkelser*
Bestemmelsen åpner for at Sikkerhetsmyndigheten kan bemyndige andre til å gjennomføre tekniske sikkerhetsundersøkelser. I disse tilfeller bør Sikkerhetsmyndigheten ha nødvendig rettslig grunnlag for å kunne be om å få oversendt rapporter fra undersøkelser. I forskrift bør det stilles nærmere kriterier og vilkår knyttet til en eventuell bemyndigelse av andre enn Sikkerhetsmyndigheten.

For å harmonisere innholdet mellom bestemmelsene om kommunikasjons- og innholdskontroll av informasjonssystemer og inntrengningstesting av skjermingsverdige informasjonssystemer, foreslår vi inntatt ordlyd som synliggjør at det etter endt TSU skal rapporteres til virksomheten.

Den som har foretatt undersøkelsen skal gi rapport om resultatet av kontrollen til virksomheten. Rapporten skal kun inneholde informasjon som er av betydning for forbedring av virksomhetens sikkerhet.

Det må også være mulig for Sikkerhetsmyndigheten å samle og analysere funn og erfaringer fra TSU til bruk i risikovurderinger, for å forbedre sikkerhetstiltak, herunder videreutvikling av metodikk for TSU, revurdering av gitte sikkerhetsmessige godkjenninger av rom og andre installasjoner, samt forbedring av rådgivningsarbeidet. En ny lov bør gi tydelig hjemmel for dette.

Til *§ 6-1 Skjermingsverdige informasjonssystemer*
I motsetning til dagens lov legger lovforslaget opp til at også visse informasjonssystemer som ikke behandler sikkerhetsgradert informasjon skal identifiseres og beskyttes, jf. første ledd bokstav a. NSM ser her at det er en utfordring knyttet til grensedragningen mellom disse systemene og systemer som vil omfattes av lovens kapittel 7 om skjermingsverdige objekter og infrastruktur. Denne grensedragningen må vurderes nærmere, vi antar at dette kan finne sin løsning gjennom presiseringer i forskrifter.

Til *§ 6-2 Beskyttelse av skjermingsverdige informasjonssystemer*
Bestemmelsen definerer de overordnede prinsipper som informasjonssystemsikkerhet skal ivareta. Inneholdet er imidlertid noe mangelfullt i forhold til hvilke kriterier som i dag legges til

grunn for god informasjonssystemsikkerhet. Første ledd bør derfor suppleres med at tiltakene også skal sikre ivaretakelse av «autentisitet, ansvarlighet og tillit».

Også på dette punkt må det kunne stilles krav til minimumstiltak jf. merknadene til § 5-2.

Til *§ 6-3 Godkjenning av skjermingsverdige informasjonssystemer*
Informasjonssystemer som behandler sikkerhetsgradert informasjon skal forhåndsgodkjennes før de tas i bruk. Informasjonssystemer som behandler informasjon av kritisk betydning for grunnleggende nasjonale funksjoner skal godkjennes, men det er ikke et krav om at dette skal gjøres før systemene tas i bruk. Det er vanskelig å se logikken i denne forskjellen. Konsekvensen kan bli at en rekke systemer som er kritiske for grunnleggende nasjonale funksjoner blir liggende ubeskyttet over tid i påvente av godkjenning. Det foreslås derfor at også informasjonssystemer som er kritiske for grunnleggende nasjonale funksjoner skal forhåndsgodkjennes før de tas i bruk.

Det er viktig med sentral oversikt over alle godkjente systemer. Dette er også nødvendig for å kunne ivareta våre forpliktelser overfor NATO. Det må derfor være en tydelig hjemmel for at Sikkerhetsmyndigheten skal kunne ha oversikt over alle godkjente systemer. Det må vurderes nærmere om det er tilstrekkelig at denne hjemmelen etableres i forskrift.

Til *§ 6-4 Overvåking av skjermingsverdige informasjonssystemer*
NSM støtter at denne bestemmelsen videreføres.

Til *§ 6-5 Kommunikasjons- og innholdskontroll av informasjonssystemer*
Hensikten med denne bestemmelsen er knyttet til å kontrollere om det kommuniseres sikkerhetsgradert informasjon i et system som ikke har den nødvendige godkjenningen for dette. Bestemmelsen bør således knyttes tettere opp mot sikkerhetsgradert informasjon. Lovforslaget definerer ikke andre informasjonskategorier og det vil således ikke være noe formelt grunnlag for å foreta vurderinger knyttet til annen informasjon som måtte oppfattes som «sensitiv». På den annen side synes formuleringen i forslaget å forutsette at man ikke kan kontrollere andre systemer enn de som er «sikkerhetsgodkjent». Dette er en uheldig begrensing som ikke samsvarer med tolkningen av dagens § 15. Erfaring tilsier at ugraderte systemer representerer den største sårbarheten for sikkerhetsgradert informasjon. Det er således av stor betydning at kommunikasjons- og innholdskontroll også i fremtiden kan gjennomføres i virksomhetenes ugraderte systemer.

For å harmonisere innholdet mellom bestemmelsene om tekniske sikkerhetsundersøkelser og inntrengningstesting av skjermingsverdige informasjonssystemer, foreslår vi inntatt ordlyd som synliggjør at det etter endt kommunikasjons- og innholdskontroll skal rapporteres til virksomheten.

Den som har foretatt kontrollen skal gi rapport om resultatet av kontrollen til virksomheten. Rapporten skal kun inneholde informasjon som er av betydning for forbedring av virksomhetens sikkerhet.

Det må også være mulig for Sikkerhetsmyndigheten å samle og analysere funn og erfaringer fra kommunikasjon- og innholdskontroll til bruk i risikovurderinger, for å forbedre sikkerhetstiltak, herunder videreutvikling av metodikk, revurdering av gitte sikkerhetsmessige

godkjenninger, samt forbedring av rådgivningsarbeidet. En ny lov bør gi tydelig hjemmel for dette.

Til *§ 6-6 Inntrengningstesting av skjermingsverdige informasjonssystemer*
Bestemmelsen legger til grunn at inntrengstesting skal være frivillig og samtykkebasert. Det bør vurderes om inntrengningsmetoder i visse tilfeller også skal kunne benyttes som ledd i Sikkerhetsmyndighetens tilsynsaktivitet. Dette bør reguleres på lovs nivå og eventuelt inntas i kapittelet om tilsynsvirksomhet.

I fjerde ledd fremgår at operasjonen skal avsluttes med en gang Sikkerhetsmyndigheten klarer å trenge inn i informasjonssystemet. Å avbryte operasjonen umiddelbart etter et vellykket inntrengingsforsøk vil bryte med dagens praksis og dramatisk redusere verdien av en inntrengningstest da man ikke vil besitte nok empiri til å avdekke eventuelle bakenforliggende svakheter. I tillegg vet man fra gjennomførte inntrengingstester at det aldri er bare en vei inn i et system. Det er avgjørende for virksomhetene å få avdekket så mange sårbarheter som mulig (helst alle), og ikke bare den første man finner. Krav om at operasjonen skal avsluttes ved vellykket inntrengning bør derfor strykes.

Til femte ledd bemerkes at det også må være mulig for Sikkerhetsmyndigheten å samle og analysere funn og erfaringer fra inntrengningstesting til bruk i risikovurderinger, for å forbedre sikkerhetstiltak, herunder videreutvikling av metodikk for inntrengningstesting, revurdering av gitte sikkerhetsmessige godkjenninger, samt forbedring av rådgivningsarbeidet. En ny lov bør gi tydelig hjemmel for dette.

Bestemmelsen åpner for det i forskrift kan fastsettes bestemmelser om at også andre enn Sikkerhetsmyndigheten kan gjennomføre inntrengningstesting av skjermingsverdige informasjonssystemer. I en slik forskrift bør det stilles nærmere kriterier og vilkår knyttet til en eventuell bemyndigelse av andre enn Sikkerhetsmyndigheten. Hvis andre enn Sikkerhetsmyndigheten gis anledning til å gjennomføre inntrengningstester bør Sikkerhetsmyndigheten også ha nødvendig rettslig grunnlag for å kunne be om å få oversendt rapporter og annen informasjon knyttet til gjennomførte undersøkelser.

Til *§ 7-1 Skjermingsverdige objekter og infrastruktur*
Det er av vesentlig betydning å holde en samlet nasjonal oversikt over skjermingsverdige objekter og infrastruktur. Det bør derfor fremgå av § 7-1 at klassifiserte objekter og infrastruktur skal meldes til Sikkerhetsmyndigheten.

Bestemmelsens ordlyd er forenklet sammenliknet med dagens § 17. Dagens bestemmelse stiller opp visse kriterier som særlig skal vurderes i utvelgelsesprosessen. NSM tror det er nyttig å ha denne typen kriterier til hjelp i utvelgelsesprosessen og mener derfor at kriteriene vurderes videreført enten på lovs nivå eller i forskrift.

Det må også sikres at objekter og infrastruktur som må skjermes på bakgrunn av internasjonale avtaler og overenskomster, slik som bakkeinfrastrukturen til satellittnavigasjonssystemet Galileo, kan utpekes som skjermingsverdig objekt eller infrastruktur.

Enkelte objekter ligger ikke nødvendigvis klart under et enkelt departements myndighetsområde. Et eksempel på dette kan f.eks. være datahaller som er kritiske på grunn av de samlede tjenester som leveres til ulike sektorer. NSM mener at lovteksten må klargjøre hvordan denne type objekter identifiseres, utpekes og klassifiseres.

Til *§ 7-2 Klassifisering*
Ordlyden i første ledd bokstav a til c er forenklet slik at det nå utelukkende vises til «*redusert funksjonalitet*». NSM legger til grunn at dette ikke innebærer en realitetsendring men at begrepet også vil favne skadeverk, ødeleggelse eller rettsstridig overtakelse.

Til *§ 7-3 Beskyttelse av objekter og infrastruktur*
Til bestemmelsens andre ledd første punkt, vil NSM bemerke at siste setningsledd ikke har selvstendig betydning. Konsekvens ved bortfall eller reduksjon av kvalitet er allerede vurdert gjennom klassifiseringen. Siste setningsledd kan derfor strykes.

Bestemmelsens tredje ledd gir hjemmel til å treffe vedtak om adgangsklarering for tilgang til skjermingsverdige objekt eller infrastruktur. I relasjon til begrepet tilgang legger NSM til grunn at dette både omfatter fysisk og logisk tilgang. Det bør vurderes om dette skal synliggjøres i bestemmelsen.

Til *§ 7-4 Testing av sikkerhetssystemer*
NSM gir sin tilslutning til at det etableres en hjemmel for testing av sikkerhetssystemer. Bestemmelsen må legge til rette for en bred virkemiddelbruk, og herunder blant annet omfatte både fysisk og logisk forsering. NSM legger til grunn at man også med hjemmel i denne bestemmelsen kan gjennomføre Tekniske sikkerhetsundersøkelser i «grunnleggende nasjonale funksjoner».

Det vises for øvrig til merknader til § 6-6.

Til Kapittel 8. Personellsikkerhet
Kapittel 8 regulerer etter forslaget autorisasjon, sikkerhetsklarering og adgangsklarering for tilgang til skjermingsverdige objekt eller infrastruktur. NSM mener at strukturen i kapittel 8 bør forbedres slik at det skilles tydeligere mellom hvilke krav som gjelder for de ulike regimene. I lys av dette bør det gis egen bestemmelse om adgangsklarering.

Etter etablert praksis er i dag informasjon i klareringssaker minimum sikkerhetsgradert BEGRENSET når den er mottatt og systematisert hos NSM og klareringsmyndighetene. I NSMs veiledning til sikkerhetsloven kapittel 6 og forskrift om personellsikkerhet er følgende uttalt på side 53: *Sammenstilling av personkontrollopplysninger knyttet til en enkeltperson vil gi indikasjoner på vedkommendes eventuelle sårbarhet, og kan potensielt utnyttes til sikkerhetstruende virksomhet. Kunnskap om hvilke personer som antas lite sårbare kan motsetningsvis lede til en mer målrettet trussel.* NSM mener dette gir uttrykk for et vesentlig prinsipp, og at det derfor bør lovfestes at systematisert og samlet personkontrollinformasjon minimum skal sikkerhetsgraderes BEGRENSET.

Til *§ 8-1 Når klarering og autorisasjon skal gjennomføres*

Til femte ledd stiller NSM spørsmål ved hensiktsmessigheten av at NATOs graderingsbetegnelser listes i bestemmelsen. Det følger av den innledende tekst at det også kan gis NATO-sikkerhetsklarering og vi mener at dette bør være tilstrekkelig.

Til *§ 8-2 Sikkerhetsautorisasjon*

NSM støtter forslaget om at virksomheten skal holde Sikkerhetsmyndigheten løpende orientert om hvilke personer som er autorisert. Dette vil imidlertid ha ressursmessige konsekvenser knyttet til teknisk tilrettelegging og løpende drift, både for Sikkerhetsmyndigheten og for den enkelte virksomhet. De sikkerhetsmessige gevinstene ved å ha oversikt over hvem som til enhver tid er autorisert antas imidlertid å oppveie de ressursmessige kostnadene. Det bør reguleres på forskriftsnivå hvordan registreringen skal gjennomføres.

Til *§ 8-3 Nedsettelse, suspensjon og tilbakekallelse av autorisasjon*

For å ha den oversikten som § 8-2 fjerde ledd legger opp til, må avgjørelse om tilbakekall, nedsettelse og suspensjon av autorisasjon også innberettes til Sikkerhetsmyndigheten.

Til *§ 8-4 Klareringsmyndigheter etter loven*

NSM vil bemerke at første ledd andre setning ikke hører naturlig hjemme i denne bestemmelsen. Setningens ordlyd er dessuten betydningsmessig lik det som følger av § 8-5 første ledd.

Til *§ 8-5 Sikkerhets- og adgangsklarering*

Det bør inntas i bestemmelsen en plikt til å innberette fattede klareringsavgjørelser til Sikkerhetsmyndigheten. Dette er nødvendig for at Sikkerhetsmyndigheten skal holde sentralisert oversikt, og er også naturlig sett i lys av § 8-6 andre ledd, og er for øvrig også dagens praksis.

NSM mener det bør vurderes å gjøre endringer i kravet i andre ledd til at sikkerhetssamtale skal gjennomføres i alle saker, med mindre dette anses som *«åpenbart unødvendig»*. En sikkerhetssamtale er ressurskrevende å gjennomføre og kan ofte også representere en belastning for vedkommende person. Kravet slik det i dag er formulert gir klareringsmyndigheten lite handlingsrom. Klareringsmyndigheten har en lovfestet plikt til å opplyse saken. Sett hen til dette mener vi at kravet til når sikkerhetssamtale skal gjennomføres kan modereres, slik at klareringsmyndigheten gis en større fleksibilitet i forhold til hvordan man velger å opplyse saken. Økt profesjonalisering gjennom en betydelig reduksjon av antallet klareringsmyndigheter må antas legge til rette for et slikt forslag.

Til tredje ledd vil NSM bemerke at politisk engasjement og annet lovlig samfunnsengasjement kan ha grenseflater mot kriterier som vil være relevant å vektlegge, særlig etter dagens § 21 bokstav c, i, k og l. Vi mener at bestemmelsen for å tydeliggjøre dette bør presiseres til:
«Politisk engasjement og annet lovlig samfunnsengasjement, herunder medlemskap i, sympati med eller aktivitet for lovlige politiske organisasjoner, skal i seg selv ikke ha betydning for vurderingen av en persons sikkerhetsmessige skikkethet.»

Fjerde ledd gir bestemmelser om vektlegging av opplysninger knyttet til nærstående. Etter ordlyden er det kun «negative» opplysninger som kan vektlegges. NSM mener dette blir for snevert. Det må være mulig å vektlegge enhver relevant opplysning som kan ha betydning for hovedpersonenes sikkerhetsmessige skikkethet. Begrepet «negative opplysninger» må tolkes som opplysninger som kan være negative for klareringsavgjørelsen, ikke nødvendigvis at det hefter noe negativt ved den nærstående. NSM vil foreslå at ordet «negative» tas ut av lovteksten for å unngå misforståelser rundt dette.

Til *§ 8-7 Gjennomføring av personkontroll*
Det bør fremgå av bestemmelsen at anmodninger om personkontroll skal fremsendes fra klareringsmyndighetene til Sikkerhetsmyndigheten. Dette representerer en kodifisering av etablert praksis, og er også konsistent med bestemmelsen i § 8-8.

Av bestemmelsens tredje ledd følger det at personkontroll i nærmere definerte tilfeller kan gjennomføres for «nærstående personer». Dette begrepet er i dag definert i personellsikkerhetsforskriftens § 1-2, nr. 5, og omfatter i personer med en familierelasjon til hovedpersonen. NSM mener denne tilnærmingen, sett hen til dagens samfunnsstrukturer, blir for snever. NSM støtter derfor utvalgets oppfatning om at begrepet bør gis et innhold slik at personkontroll kan gjennomføres for alle de personer som har en reell påvirkningsmulighet på vedkommende sikkerhetsmessige skikkethet.

NSM legger til grunn at det innenfor rammen av tredje ledd fortsatt vil være mulig i særlige tilfeller å gjennomføre personkontroll av nærstående der det er anmodet om sikkerhetsklarering på nivå KONFIDENSIELT. Det bør vurderes om dette også tydeligere bør fremgå av lovteksten.

Til fjerde ledd vil NSM bemerke at hjemmelen til å innhente opplysninger fra «andre kilder» må forstås slik at Sikkerhetsmyndigheten også kan innhente opplysninger fra offentlige eller kommersielt tilgjengelige kilder. NSM legger til grunn at begrepet «offentlige registre» også omfatter opplysninger som virksomheten lagrer på annen måte, eksempelvis i elektroniske saksarkiv ol.

Etter sjette ledd skal opplysninger gitt til klareringsmyndigheten i forbindelse med personkontroll, ikke benyttes til andre formål enn vurdering av klarering. Bestemmelsen bør ha en henvisning til unntaket i § 8-12.

NSM mener videre at det bør gis en klar hjemmel for Sikkerhetsmyndigheten og klareringsmyndighetene til å benytte opplysningene i den grad det er nødvendig for å ivareta ansvar og oppgaver innen personellsikkerhet, herunder tilsyn, utvikling av personellsikkerhetsfaget og -tiltak, informasjon, råd og veiledning, samt informasjon om trusselvurderinger og risikohåndtering.

I niende ledd er det en feil henvising. Riktig henvisning skal være § 8-5 tredje ledd andre punkt.

Til *§ 8-9 Bruk av vilkår og stillingsklarering*
NSM fremholder det som positivt at muligheten for stillingsklarering lovfestes.

Til *§ 8-10 Klarering av personer som ikke er norske statsborgere*

Et grunnleggende prinsipp når det gjelder sikkerhetsklarering er at den som skal klareres må forutsettes å være lojal mot norske sikkerhetsmessige interesser. En slik lojalitet fordrer etter NSMs oppfatning en viss tilknytning til Norge. Etter sikkerhetslovens § 22 gis i dag klarering av utenlandske statsborgere etter en «vurdering av hjemlandets sikkerhetsmessige betydning og vedkommendes tilknytning til hjemlandet og Norge». Forslaget om å endre ordlyden til «..vedkommendes *eventuelle* tilknytning til Norge» innebærer en *vesentlig* oppmyking av adgangen til å klarere utenlandske statsborgere uten at de sikkerhetsmessige konsekvenser kan sees utredet i lovforslaget. NSM mener at det allerede i dag ligger til rette for en skjønnsmessig praktisering av gjeldende bestemmelse, og at graden av tilknytning til Norge og betydningen av denne, også etter gjeldende regelverk undergis en individuell og skjønnsmessig vurdering som forutsettes å ivareta både sikkerheten og rettssikkerheten på en god måte. NSM mener derfor at dagens ordlyd på dette punkt bør videreføres.

I den utstrekning det skal være mulig å klarere en person uten noen form for tilknytning til Norge bør dette bare skje unntaksvis, og basert på en dispensasjon gitt av Sikkerhetsmyndigheten. Det bør i så fall etableres en dispensasjonshjemmel med utgangspunkt i en ordlyd videreført fra dagens § 22.

For å unngå misforståelse knyttet til klarering av personer som ikke er norske statsborgere bør bestemmelsen knyttes tettere til de generelle krav som gjelder for personer i § 8-5. Dette kan gjøres ved å tilføye som siste setningsledd i første ledd andre setning:

(…), jf. § 8-5.

Videre bør ordlyden endres slik at det fremgår at disse kriteriene kommer i tillegg til kriterier som vil følge av og i medhold av § 8-5. Første ledd tredje setning bør derfor lyde:

I vurderingen skal det i tillegg legges vekt på(…)

Til *§ 8-11 Varslingsplikt*

NSM støtter at varslingsplikten blir tydeliggjort i en egen paragraf, samt at autorisasjonsmyndigheten nå gis en plikt til å varsle klareringsmyndigheten dersom forholdet antas å kunne få betydning for vedkommendes klarering.

Til *§ 8-12 Informasjonstilgang for Politiets sikkerhetstjeneste*

NSM merker seg at forslaget i Sikkerhetsfaglig råd om å legge til rette for målrettet informasjonstilgang med Politiets Sikkerhetstjeneste (PST) er tatt videre av utvalget. NSM antar at det i denne forbindelse også vil være hensiktsmessig at hjemmelsgrunnlaget også omfatter å gi PST informasjon om vedkommendes autorisasjonsstatus som en pekepinn på hvilket potensielt skadeomfang det kan være snakk om.

Bestemmelsen bygger på det utgangspunkt at informasjon gis etter forespørsel fra PST. Innen de rammer som følger av bestemmelsen bør Sikkerhetsmyndigheten også kunne gi denne type informasjon av eget tiltak, av hensyn til at slik informasjon raskt kan komme PST i hende.

Sikkerhetsmyndigheten bør imidlertid i saker hvor det deles informasjon i medhold av § 8-12 orienteres i nødvendig grad om de forebyggende tiltak som PST gjennomfører, slik at den daglige sikkerhetsmessige ledelse av vedkommende ikke kommer i konflikt med disse tiltakene. NSM antar at dette kan løses gjennom forskrift til bestemmelsen.

I forlengelsen av denne problematikken vil NSM påpeke viktigheten av det legges til rette for at PST generelt og fortløpende informerer Sikkerhetsmyndigheten om alle nye forhold som er relevante for sikkerhetsklarerte personers sikkerhetsmessige skikkethet. Dette bør vurderes i det videre lovarbeidet.

Det er viktig at man i det videre arbeidet tar hensyn til at sikkerhetsmyndigheten og PST har ulike formål med sin virksomhet og at begges formål blir ivaretatt på en god måte.

Til *§ 8-13 Begrunnelse og underretning*

NSM mener det bør tas inn en egen hjemmel til å unnta *opplysninger om sikkerhetstjenestens metoder* i opplistingen av hvilke forhold som kan unntas fra begrunnelse og innsyn. Innsyn i enkelte av de metoder som klareringsmyndighetene benytter for å opplyse en sak vil kunne skade fremtidige muligheter for å opplyse tilsvarende saker på en sannferdig måte. Inngående kjennskap til enkelte metoder kan medføre at det blir mulig å lage oppskrifter for hvordan man skal kunne manipulere klareringsmyndigheten til å fatte uriktige avgjørelser.

På denne bakgrunn foreslås en ny bokstav e i bestemmelsens andre ledd som angår sikkerhetstjenestens metoder.

Til *§ 8-14 Innsyn*

Bestemmelsens siste ledd bør harmoniseres med dagens praksis hvor innsyn i opptak og referat fra sikkerhetssamtale kun gis ved gjennomsyn hos klareringsmyndigheten. Dette er begrunnet i sikkerhetsmessige forhold og praksisen ble forutsatt ved innføringen av retten til innsyn, jf. Ot.prp. nr. 59 2004-2005, merknad til ny § 25a.

NSM foreslår på denne bakgrunn at tredje ledd endres til: «*Den som har krav på innsyn skal på anmodning gis kopi av dokumentet. Innsyn i opptak og referat fra sikkerhetssamtale gis ved gjennomsyn hos klareringsmyndigheten».*

Til *§ 8-15 Oversendelse av sak til særskilt oppnevnt advokat*

Denne bestemmelsen ble innført ved lovendring i 2005, og var ment å styrke rettssikkerheten til den enkelte. Tidligere var det angitt at det var Forsvarsdepartementet som skulle oppnevne en gruppe advokater for dette formålet. Gitt bruken av begrepet «departementet» og dagens ansvarsdeling er det ikke klart om FD fortsatt skal ha denne rollen. Dette bør tydeliggjøres.

Til *§ 8-16 Klage*

NSM har som klage- og tilsynsmyndighet erfart at reguleringen klagesaksbehandling dels i sikkerhetsloven og dels i forvaltningsloven skaper betydelig usikkerhet knyttet til saksbehandlingen av klagesaker. NSM har på denne bakgrunn tidligere fremmet forslag om å samle all regulering av klage innenfor personellsikkerhetsområdet i egne bestemmelser under sikkerhetsloven.

NSM foreslår at henvisningen til forvaltningsloven erstattes av en bestemmelse som gir hjemmel for å gi utfyllende bestemmelser om klage i forskrifter til ny lov om forebyggende nasjonal sikkerhet.

Til *§ 9-1 Sikkerhetsgradert anskaffelse*
NSM merker seg at utvalget i stor grad foreslår en videreføring av dagens regelverk når det gjelder Sikkerhetsgraderte anskaffelser. NSM mener at det er et stort behov for regimet, og støtter en videreføring av regelverket. Dagens regime er et veletablert regime, som først og fremst sikrer at nødvendig regelverk kommer til anvendelse på private aktører, for at disse skal kunne få tilgang til sikkerhetsgradert informasjon. Det bør vurderes å tydeliggjøre i lovforslaget at eventuelle leverandører må kunne tilfredsstille alle relevante krav i loven for å kunne få tilgang til sikkerhetsgradert informasjon/skjermingsverdig objekt og infrastruktur, før man kan tildeles en gradert kontrakt.

NSM ser videre at en viktig del av dette regimet ikke er tydelig presisert hverken i det eksisterende regelverket eller i forslaget til ny lov. Dette gjelder den internasjonale dimensjonen av regimet. Det er gjennom dette regelverket at man sikrer norske leverandørers tilgang til det internasjonale markedet som involverer utenlandsk sikkerhetsgradert informasjon, og gjør det mulig for norske virksomheter å benytte leverandører fra utlandet dersom det er behov for dette.

De internasjonale sikkerhetsgraderte anskaffelser er nært knyttet opp til bilaterale og multilaterale sikkerhetsavtaler som Norge har inngått med andre stater/organisasjoner. NSM mener at det er viktig at også denne delen av regimet reflekteres på en god måte i regelverket. Det bør vurderes om denne dimensjonen bør tydeliggjøres i lovforslaget eller om det er tilstrekkelig å beskrive dette nærmere i en lovproposisjon. Nærmere konkrete bestemmelser må uansett utformes i forskrifts form.

Til *§ 9-3 Leverandørklarering*
I Sikkerhetsfaglig råd anførte NSM at det er et stort behov for å styrke fagmyndighetsrollen i NSM, for å sikre at prosessene rundt sikkerhetsgraderte anskaffelser er gode og sikre nok. NSM bruker i dag mesteparten av sine ressurser på området til å fatte vedtak om leverandørklareringer. Sikkerhetsloven åpner i dag ikke for at andre enn NSM kan fatte vedtak om leverandørklarering. Både nåværende fagmiljøer for sikkerhetsgraderte anskaffelser i Forsvaret og Forsvarsbygg, samt de foreslått opprettede klareringsmyndighetene på militær og sivil side, kan være aktuelle med tanke på utøvelse av myndighet til å gi leverandørklareringer. Ressursene i NSM som frigjøres ved en slik omlegging bør refokuseres til kontroll og utvikling innen området, herunder utvikle regelverk og veiledninger.

På bakgrunn av dette anbefalte NSM følgende tiltak i Sikkerhetsfaglig råd:
Forsvarsdepartementet bør fremme et forslag om at sikkerhetsloven endres slik at Kongen kan utpeke klareringsmyndigheter og klageinstans for saker om leverandørklarering og andre myndighetsavgjørelser på området.

NSM registrerer at utvalget ikke har fulgt opp denne anbefalingen, men anbefaler at det gjøre en fornyet vurdering slik at det åpnes for at klareringsmyndighet for leverandører også kan legges til andre enn Sikkerhetsmyndigheten.

I bestemmelsens andre ledd brukes begrepet *«anskaffelsesmyndigheten»*. NSM legger til grunn at alle virksomheter som blir omfattet av lovforslaget vil kunne gjennomføre sikkerhetsgraderte anskaffelser, herunder også private rettssubjekter. I denne kontekst synes ikke begrepet «anskaffelsesmyndigheten» helt treffende. NSM foreslår derfor at det heller benyttes formuleringen *«virksomheten som gjennomfører anskaffelsen».*

Til *§ 9-4 Varslingsplikt og myndighet til å fatte vedtak ved anskaffelser til skjermingsverdig objekt og infrastruktur*

NSM foreslår at det i første ledd foretas en presisering slik at første punkt blir lydende *«Ved anskaffelser til skjermingsverdig objekt eller infrastruktur skal virksomheten som foretar anskaffelsen gjennomføre en risikovurdering»*

Til *§ 10-1 Eierskapskontroll*

NSM slutter seg til utvalgets vurderinger knyttet til behovet for en bestemmelse om eierskapskontroll. Behovet for en slik mekanisme er tidligere tatt opp av NSM, første gang i daværende FO/S sin høringsuttalelse i forbindelse med opphevelsen av ervervsloven.

NSM støtter i hovedsak utvalgets forslag til utforming av lovbestemmelsen. Vi stiller oss imidlertid noe undrende til at det etter bestemmelsens første ledd er det utenlandske rettssubjekt som skal sende melding og ikke den norske virksomheten selv.

Til *§ 11-2 Tvangsmulkt og § 11-3 Overtredelsesgebyr*

NSM har erfart at pålegg om å lukke avvik ikke alltid etterkommes av virksomheten. I dag har NSM få virkemidler i disse tilfellene. Det er derfor positivt at nye virkemidler foreslås, og NSM støtter at det innføres et hjemmelsgrunnlag for tvangsmulkt og overtredelsesgebyr.

Til *§ 12-1 Ikrafttredelse*

Lovens virkeområde utvides i forhold til dagens sikkerhetslov, jf. introduksjonen av begrepet grunnleggende nasjonale funksjoner. Loven vil i tillegg til å omfatte sikkerhetsgradert informasjon og skjermingsverdige objekter også omfatte informasjonssystemer er skjermingsverdige av andre grunner, samt infrastruktur. På den annen side vil ikke nødvendigvis alle dagens utpekte objekter i fremtiden væres skjermingsverdige i henhold til loven. Det må utformes hensiktsmessige og realistiske overgangsbestemmelser for å fange opp disse endringene.

5 Områder som ikke dekkes av lovforslaget

Ut over de forslag som er fremmet av Sikkerhetsutvalget, ser NSM at det er behov for å vurdere reguleringsbestemmelser på enkelte områder som ikke er utredet av utvalget. Dette gjelder følgende områder:

Hjemmel for sårbarhetskartlegging

NSM tilbyr i dag en tjeneste for kartlegging av offentlig tilgjengelige sårbarheter i IKT-systemer tilknyttet internett, - Alvis nor. I dag er denne tjenesten basert på samtykke fra den enkelte systemeier, og antallet tilknyttede virksomheter lavt. Erfaring viser at prosessen med å innhente samtykke er krevende. Dette medfører at NSM ikke har noen god oversikt over sårbarheter i norsk samfunnskritisk IKT-infrastruktur. Det bør derfor vurderes om NSM skal gis hjemmel til å utføre denne type sårbarhetskartlegginger uten samtykke.

Bruk av tredjepart

NSM har etablert en kvalitetsordning for bruk av tredjeparter innen hendelseshåndtering. Det vurderes om denne ordningen også på sikt skal utvides til andre sikkerhetsområder. Det er i dag ikke et formelt hjemmelsgrunnlag for denne ordningen, og NSM har heller ikke mulighet for å få dekket sine utgifter knyttet til forvaltningen. NSM mener det bør vurderes en lovhjemmel for ordningen, herunder et hjemmelsgrunnlag for å kunne kreve gebyr.

Obligatorisk tilknytning til VDI systemet for visse virksomheter

I Sikkerhetsfaglig råd ble det fremmet forslag om obligatorisk tilknytning til VDI systemet for virksomheter med samfunnsviktig IKT-infrastruktur og funksjoner. Sikkerhetsutvalget konkluderer ikke i denne saken, men påpeker at spørsmålet om obligatorisk tilknytning til VDI må sees i sammenheng med en fremtidig finansieringsmodell for VDI, og fremhever viktigheten av at et slikt utredningsarbeid igangsettes raskt. NSM mener derfor at det bør gjøres en snarlig vurdering av om det skal gis en hjemmel for obligatorisk tilknytning til VDI-systemet.

Kjetil Nilsen
Direktør