NASJONAL
SIKKERHETSMYNDIGHET

| Vår saksbehandler | Vår dato | Vår referanse |
|---|---|---|
| Stab | 2018-09-28 | A03 - S:18/03321-1 |
| | Deres dato | Deres referanse |
| | Antall vedlegg | Side 1 av 19 |

Til
Forsvarsdepartementet
Postboks 8126 Dep
0032 OSLO
Norge

# Høringsuttalelse til høringsnotat om forskrifter til ny sikkerhetslov

Nasjonal sikkerhetsmyndighet (NSM) viser til departementets brev av 2.7. 2018 hvor høringsnotat til forskrifter til ny sikkerhetslov sendes ut på høring.

Nedenfor følger NSMs uttalelse. Høringsuttalelsen er strukturert i en del som inneholder noen overordnede betraktninger knyttet til forslaget, samt en del hvor vi gir konkrete kommentarer til de enkelte bestemmelser.

## 1 Overordnede betraktninger

### 1.1 Inndelingen av forskriftene

Høringsnotatet foreslår tre forskrifter, - forskrift om myndighetenes roller og ansvar for nasjonal sikkerhet, forskrift om virksomhetenes arbeid med forebyggende sikkerhet og forskrift om klarering av leverandører og personell.

NSM er av den oppfatning at valgt forskriftsstruktur er uheldig. Strukturen bryter med lovens systematikk. Dette gjør regelverksanvendelsen krevende og lite brukervennlig. I tillegg til å måtte lese lov og forskrift i sammenheng, må brukeren nå finne frem i tre ulike forskrifter, samt en lov, med en ulik strukturell tilnærming. Det er NSMs oppfatning at regelverket hadde vært mer tilgjengelig om lov og forskrift fulgte samme strukturelle inndeling.

NSM mener at som et minimum bør forskrift om virksomhetens arbeid med forebyggende sikkerhet og forskrift om klarering av personell vurderes slått sammen. Veiledninger kan også bidra til å forenkle denne utfordringen.

### 1.2 Digitalisering og automatisering

Samfunnet digitaliseres i høy hastighet. NSM vil påpeke at det er viktig at forskriftene utformes på en slik måte at også sikkerhetsarbeidet kan bli en del av denne utviklingen. Flere av bestemmelsene i forskriftene forutsetter at det skal gis nærmere opplistede opplysninger på «skjema». Dette gjelder for eksempel ved sikkerhetsklarering av personell og leverandører. Ett av prinsippene for digitalisering av offentlig sektor er at myndighetene ikke skal spørre om noe myndighetene vet fra før. NSM mener det er viktig at

**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

forskriftsbestemmelsene på dette området utformes på en slik måte at de ikke er til hinder for en fremtidig digitalisering og automatisering.

## 1.3 Roller og ansvar

Ny lov om nasjonal sikkerhet tillegger de enkelte departementene og tilsynsorganer i sektorene en mer omfattende rolle enn disse har etter dagens lov. Samtidig videreføres en sikkerhetsmyndighet med et tverrsektorielt ansvar. I ny lov og i utkastet til forskrifter er det valgt en reguleringsteknikk som oppstiller funksjonelle krav til sikkerhet.

NSM støtter denne tilnærmingen, men vil påpeke at den nødvendiggjør at hvilket ansvar som tilligger sektorene og hvilket ansvar som tilligger sikkerhetsmyndigheten er tydelig definert. Tilnærmingen med funksjonelle krav fordrer også høy sikkerhetsfaglig kompetanse i alle ledd.

Loven og forskriftsutkastet legger opp til at virksomheter og sektorer selv skal vurdere egen risiko og treffe nødvendige tiltak innenfor rammen av forskriftenes sikkerhetsmål. Dette kombinert med en forskrift med funksjonelle krav som åpner for en dynamiske og løpende tolkning av de ulike sikkerhetsmålene opp mot ny teknologi vil kunne skape ulike sikkerhetsnivåer på tvers av ulike sektorer og virksomheter.

For å oppnå en enhetlig implementering av regelverket på tvers av sektorer er det sentral at det etableres en sterk sikkerhetsmyndighet, som kan bidra til at en enhetlig forvaltningspraksis. Dette påpekte NSM i høringsuttalelsen til NOU 2016:19, og våre merknader på dette området er i vesentlig grad ivaretatt i ny lov om nasjonal forebyggende sikkerhet.

Sikkerhetsmyndighetens ansvar fremgår av ny lov om nasjonal forebyggende sikkerhet § 2-2. NSM legger til grunn at sikkerhetsmyndigheten med hjemmel i denne bestemmelsen vil kunne innhente den informasjon som er nødvendig for å kunne etablere en nasjonal oversikt over sikkerhetstilstanden, for å kunne vurdere om regelverket er enhetlig implementert på tvers av sektorene, og ivareta de øvrige oppgaver loven og forskriftsutkastet tillegger sikkerhetsmyndigheten. Det legges videre til grunn at bestemmelsen innebærer en påleggskompetanse for de tilfeller hvor det er behov for å innhente informasjon for å ivareta disse oppgavene.

Informasjon, råd, veiledning om forebyggende sikkerhetsarbeid vil være sentralt for å implementere et regelverk som stiller funksjonelle krav. Sektormyndighetene vil ha hovedansvaret for implementering av tiltak i sektor. Vil legger imidlertid til grunn at sikkerhetsmyndigheten, som nasjonal fagmyndighet etter lovens § 2-2, første ledd bokstav d og h, vil ha et særskilt ansvar for utforming av forvaltningspraksis for å sikre en enhetlig implementering av regelverket gjennom veiledninger på tvers av sektorene.

## 1.4 Forsvarlig sikkerhet

Departementet ber i høringsnotatet om tilbakemelding på innretningen på de krav som stilles til hvordan en virksomhet kan beskytte sine skjermingsverdige verdier på en slik måte at kravet til forsvarlig sikkerhetsnivå oppnås.

NSM støtter innretningen, men ønsker å påpeke at fortolkningen av de funksjonelle kravene vil måtte utvikles over tid igjennom forvaltningspraksis. Sikkerhetsmyndigheten på tversektorielt nivå, og tilsynsmyndighetene i den enkelte sektor, vil være viktige premissleverandører for hvordan kravet til forsvarlig sikkerhetsnivå skal .

## 1.5 Varslingssystem for digital infrastruktur

Høringsutkastet viderefører dagens ordning med en tilknytning til Varslingssystem for digital infrastruktur på frivillig basis. Departementet har bedt om høringsinstansenes tilbakemelding på om sikkerhetsmyndigheten skal gis mulighet til å pålegge virksomheter å være tilknyttet VDI og hvilke rammer en slik påleggskompetanse bør ha.

Dagens VDI dekning er etter NSMs oppfatning ikke god nok. Dagens modell som er basert på frivillighet og at tilknyttede virksomheter betaler en årlig medlemsavgift gir ikke en tilfredsstillende dekningsgrad i alle sektorer.

NSM mener at sikring av grunnleggende nasjonale funksjoner og nasjonale sikkerhetsinteresser ikke kan være opp til virksomhetenes betalingsevne og -vilje. Vi mener derfor at det er helt nødvendig at finansieringsmodellen endres slik at kostnadene fullfinansieres over statsbudsjettet, og at det etableres en hjemmel for å pålegge virksomheter å være tilknyttet VDI. Det vises for øvrig til mer utførlige kommentarer under merknadene til § 12 i myndighetsforskriften.

## 1.6 Kompetanse og ressurser

Departementer, NSM, sektormyndigheter og virksomheter vil alle stå overfor en rekke utfordringer knyttet til regelverkets implementering. En rekke komplekse prosesser skal gjennomføres blant annet knyttet til å identifisere og utvelge virksomheter som skal være omfattet av loven, vurdering av forsvarlig sikkerhetsnivå, gjennomføring av risiko og sårbarhetsanalyse, identifisering og implementering av tilstrekkelige sikringstiltak, og utvikling av metodikk for gjennomføring av tilsyn.

Som NSM også påpekte i høringsuttalelsen til NOU 2016:19 vil nytt regelverk være krevende å gjennomføre og vil fordre betydelig ressursinnsats, kompetanse og vilje til gjennomføring hos både NSM, sektormyndigheter og virksomheter.

Implementering av regelverket vil ta tid og medføre kostnader. Implementeringen fordrer også på mange områder en kompetanse som i dag er mangelvare, og som vil ta tid å bygge. Det er ikke realistisk å tro at tilstrekkelig kompetanse og ressurser vil være på plass innen 1.1.2019.

# 2 Merknader til de enkelte forskriftene

## 2.1 Merknader til forskrift om myndighetens roller og ansvar for nasjonal sikkerhet (myndighetsforskriften)

**Til § 5 Fellesregler for tekniske sikkerhetsundersøkelser, inntrengningstesting, testing av sikkerhetstiltak og kommunikasjons – og innholdskontroll av informasjonssystemer.**

Departementet foreslår at resultatet fra disse undersøkelsene skal rapporteres til «myndigheten som fører tilsyn etter loven». Tekniske sikkerhetsundersøkelser, inntrengningstesting, testing av sikkerhetstiltak og kommunikasjons- og innholdskontroll av informasjonssystemer baserer seg på en avtale mellom NSM og virksomheten som skal testes, og er avhengig av virksomhetens samtykke. Tillitt mellom NSM og virksomheten er

kritisk for gjennomføringen. Denne tilliten baserer seg blant annet på at funn fra testene er virksomhetens eie og kun benyttes i henhold til formålet kontrollen krever. Rapporteringsforpliktelser som går ut over lovens krav til sikkerhetsmyndighetens rapport til virksomheten bør av den grunn avtalefestes. Den foreslåtte rapporteringsplikten synes å gå lengre enn hva som følger av lovens bestemmelser, og hva forarbeidene forutsetter. Forarbeidene viser til at i de tilfeller det oppdages alvorlige avvik så bør dette videreformidles til sektordepartementet. Det antas forutsetningsvis å følge av dette at det i de tilfeller hvor avvikene ikke er alvorlige er opp til virksomheten selv å avgjøre informasjonsdeling.

NSM foreslår at bestemmelsens første ledd endres til:

*Den som gjennomfører tester, kontroller og undersøkelser som nevnt i sikkerhetsloven §§ 5-5, 6-5, 6-6 og 7-4 skal rapportere resultatene til virksomheten og andre innenfor rammen av det som er avtalt mellom partene. Rapporten skal ikke unødig inneholde informasjon som identifiserer enkeltpersoner som måtte ha begått sikkerhetsbrudd.*

### Til § 7 Om kryptotjenester

Et sentralt prinsipp for forsvarlig forvaltning av kryptomateriell er en sentralisert regnskapsmessig kontroll med materiellet. Etter forskriftsutkastet § 7 at NSM skal ha «oversikt» over det nasjonale kryptoregnskapet. Dette fremstår som for svakt. Vi mener det er helt nødvendig at NSM skal ha *kontroll* over det nasjonale kryptoregnskapet for å ha nødvendige fullmakter overfor kryptoholdere og for å ivareta det lovpålagte kravet om nasjonalt forvalteransvar for kryptomateriell. Her er det viktig å understreke at overnasjonalt regelverk som eksempelvis NATO og EU regelverk forutsetter slik kontroll.

NSM foreslår at første ledd endres til:

*Nasjonal sikkerhetsmyndighet skal ivareta rollen som nasjonal distribusjonsmyndighet for nasjonalt kryptomateriell mottatt fra fremmede stater og internasjonale organisasjoner, og skal ha regnskapsmessig kontroll over kryptomateriell. Med kryptomateriell menes kryptodokumenter, kryptonøkler og kryptoutstyr.*

### Til § 11 Unntak fra krav om sikkerhetsklarering og autorisasjon

Departementet ber om høringsinstansenes syn på behovet for og hensiktsmessigheten av den unntaksbestemmelsen som er foreslått i § 11. NSM vil første bemerke at høringsnotatets omtale av unntaksbestemmelsen i første avsnitt under pkt. 4.5.4 gir et noe et feilaktig inntrykk av hvilke tilfeller det er aktuelt å benytte unntaksbestemmelsen. Det nevnes her avtaler stat-til-stat som regulerer tilgangen til informasjon. NSM kan ikke se at det i *disse* tilfellene vil være nødvendig å benytte en unntaksbestemmelse fra kravet om sikkerhetsklarering, idet avtalene regulerer hvordan informasjonsutvekslingen skal foregå.

Når det gjelder selve forslaget, mener NSM det er behov for en slik bestemmelse, men presiserer at unntak kun kan skje i særskilte tilfeller og etter en forutgående risikovurdering hvor det forutsettes at det respektive sektordepartement bidrar inn i vurderingen av om det foreligger et særlig behov etter bestemmelsens andre ledd.

## Til § 12 Utøvelse av nasjonal responsfunksjon for alvorlige digitale angrep og nasjonalt varslingssystem for digital infrastruktur.

I § 12 fastsettes at det er NSM som skal drive responsfunksjonen og varslingssystemet for digital infrastruktur (VDI). Dette er en videreføring av en oppgave NSM ivaretar i dag, jf. sikkerhetsloven § 9e. Høringsutkastet legger opp til at tilknytning til VDI baseres på frivillighet, og hvor NSM inngår avtaler med hver enkelt virksomhet som ønsker å være tilknyttet. Departementet har imidlertid bedt om tilbakemelding på om NSM skal gis mulighet til å pålegge virksomheter å være tilknyttet VDI og hvilke rammer en slik påleggskompetanse bør ha.

VDIs evne til å oppdage hendelser i norsk kritisk infrastruktur er et gjennomprøvd konsept som har vært operativ i nesten 20 år. Gjennom disse årene har VDI plattformen optimalisert evnen til å detektere alvorlige cyberhendelser. VDI er en meget god løsningen i balansen mellom myndighetens behov for deteksjon i kritisk infrastruktur og behandling av personopplysninger. I dag er det en jevn etterspørsel fra ulike aktører om tilkobling til VDI. Utfordringen er imidlertid at etterspørselen etter tilkobling ikke gjenspeiler det som vil være en korrekt dekningsgrad i forhold til grunnleggende nasjonale funksjoner. I dagens modell er det i enkelte sektorer en underdekning, og NSM ser omfattende aktivitet som synliggjør store mørketall som ikke blir fanget opp pga. for dårlig dekningsgrad.

Det er derfor avgjørende at tilknytting til VDI underlegges en modell som vil gi en dekningsgrad som omfatter hele bilde av kritisk infrastruktur. Dette vil sikre evne til varsling, og et oppdatert situasjonsbilde i cyber, som premiss for politiske beslutninger og politikkutforming.

For å oppnå en tilfredsstillende dekningsgrad i alle relevante sektorer mener NSM at det er helt nødvendig at finansieringsordningen endres, slik at VDI-systemet fullfinansieres over statsbudsjettet, og at NSM gis påleggskompetanse i tilfeller hvor det er nødvendig at en virksomhet knyttes opp mot VDI-systemet. NSM ser det som naturlig at en eventuell påleggskompetanse knyttes opp til virksomheter som er underlagt sikkerhetsloven og da spesielt opp mot virksomheter som har betydning for grunnleggende nasjonale funksjoner.

## Til § 13 Informasjonsbehandling og - deling

Bestemmelsen er ment å gi NSM hjemmel til å dele informasjon med partene i FCKS når dette er av betydning for å sikre nasjonale sikkerhetsinteresser. Det vises i høringsnotatet til at hensikten er å sikre informasjonsflyt mellom de hemmelige tjenestene og på den måten bidra til å oppfylle formålet med FCKS.

NSM har sett et klart behov for denne bestemmelsen igjennom håndtering av alvorlige dataangrep der rask flyt av informasjon mellom tjenestene kan være av stor betydning for å ivareta forbyggende sikkerhet og bekjempe trussel aktører. I disse tilfellene vil det også være behov for informasjonsdeling med andre aktører som har en rolle i tilknytning til hendelsen.

I forslaget til forskriftsbestemmelse stilles det imidlertid som krav at det må være inngått en avtale etter § 56 i virksomhetsforskriften som at informasjon kan deles. § 56 regulerer inngåelse av VDI -avtale mellom NSM og virksomheten. Bestemmelsen kan dermed leses slik at det bare kan deles informasjon der en hendelse oppstår ved en virksomhet som er tilknyttet VDI. Det ekskluderer deling av informasjon med FCKS når det er alvorlige dataangrep som treffer virksomheter som ikke er tilknyttet VDI, men hvor NSM bistår virksomheten f eks gjennom teknisk analyse av lagringsmedier. Slike angrep kan ha stor

betydning for nasjonale sikkerhetsinteresser og bestemmelsen bør ikke skille mellom angrep som treffer virksomheter som er tilknyttet VDI og virksomheter som ikke er tilknyttet VDI. I tillegg ser NSM et stort behov for at bestemmelsen utvides til også å gjelde deling av informasjon med andre aktører som har behov for informasjonen i forbindelse med en hendelse.

NSM foreslår at første ledd endres til:

*Nasjonal sikkerhetsmyndighet kan dele informasjon med partene i Felles cyberkoordingerssenter og til andre aktører som har behov i forbindelse med en konkret hendelse.*

**Til § 15 Avtale om samarbeid mellom Nasjonal sikkerhetsmyndighet og andre myndigheter med tilsynsansvar**

Utkastet til forskriftsbestemmelse synes i bokstav b å gå lenger enn loven når det gjelder å pålegge NSM en plikt til at tilsynspersonell fra sektormyndigheter har den nødvendige kompetansen. NSM vil påpeke at enhver sektor, og et hvert organ, selv har primæransvar for egen kompetanse. NSM sin rolle er i så måte understøttende. Bestemmelsen reflekterer i liten utstrekning dette prinsipielle utgangspunktet.

I merknaden til bestemmelsen i høringsnotatet fremgår det at «*NSM skal sikre at sektormyndigheten kan opparbeide seg og vedlikeholde den nødvendige kompetansen gjennom opplæring og veiledning av sektormyndigheten innen sikkerhetsfaget og NSMs kriterier for tilsyn.*» Denne formuleringen innebærer at NSM bærer hele ansvaret for at sektormyndigheten er kompetent. Det vil være urimelig at NSM skal bære hele denne byrden. NSM kan heller ikke se at tilsvarende sterke formulering er benyttet i forarbeidene til loven. I forarbeidene til loven benyttes derimot uttrykk som må oppfattes som en tilretteleggingsplikt og ikke en plikt til å bære hele ansvaret for sektormyndighetens kompetanse.

Etter lovens § 3-2 tredje ledd og merknader knyttet til denne bestemmelsen i forarbeidene fremgår det at NSM kan medvirke til sektormyndighetenes tilsyn. Formålet med slik medvirkning er todelt. For det første kan slik medvirkning skje der er nødvendig av hensyn til sikkerhetsmyndigheten oppgaveløsning. For det andre kan medvirkning være begrunnet i at sektormyndighetene har et behov for bistand. Av forskriftsbestemmelsen bokstav c med merknader synes kun sistnevnte hensyn å være ivaretatt. NSM foreslår at opplistingen i første ledd endres til også å omfatte førstnevnte hensyn.

NSM vil også påpeke at en forutsetning for at det kan gjøres avtaler i henhold til bokstav g er at NSM kan bemyndige andre som godkjenning- og dispensasjonsmyndigheter. Vi viser her til vår kommentar til virksomhetsforskriften § 47.

NSM foreslår at første ledd endres til:

*Avtale om samarbeid mellom sikkerhetsmyndigheten og sektormyndighet jf. sikkerhetsloven § 3-2 første ledd, skal som et minimum omhandle:*

*a) Kriterier som skal ligge til grunn for tilsynet*
*b) Opplæring og veiledning av sektormyndighetene*
*c) Forberedelse og gjennomføring av tilsyn*
*d) Deling av relevant informasjon om trusselbildet og risiko med tilsynsmyndigheten*

e) *Tilsynsmyndighetens rapportering til Nasjonal sikkerhetsmyndighet om planlagte tilsyn og gjennomførte tilsyn*
f) *Varsling, jf. sikkerhetsloven § 4-5*
g) *Utøvelse av godkjennings- og dispensasjonsmyndighet i sektoren*
h) *Sektormyndighetens deling av kompetanse med Nasjonal sikkerhetsmyndighet*

## 2.2 Merknader til forskrift om virksomhetenes arbeids med forebyggende sikkerhet (virksomhetsforskriften)

### Til § 11 Plikt til å vurdere risiko

Virksomhetens plikt til risikovurdering følger av lovens § 4-2. Første ledd i bestemmelsen bør derfor vise til lovens § 4-2 og ikke forskriftens § 4. Slik bestemmelsen står nå er den egent til å skape uklarhet. Bestemmelsen kan lese dithen at § 11 ikke er ment til å omhandle risikovurderinger etter § 4-2. Vi legger til grunn at dette ikke har vært departementets intensjon, i og med at siste ledd i bestemmelsen viser til § 4-2. Det bør i denne sammenheng også tas inn en referanse til lovens § 4-2 i forskriftens § 4.

NSM foreslår at første ledd endres til:

*Når virksomheter vurderer risiko etter lovens § 4-2 skal den ta hensyn til:*
*a) hvilken sikkerhetstruende virksomhet de skjermingsverdige verdiene kan bli utsatt for,*
*b) hvilke sårbarheter som er knyttet til de skjermingsverdige verdiene*
*c) i hvilken grad virksomheten er avhengig av andre virksomheter for å fungere som den skal.*

Videre bør siste ledd i bestemmelsen endres til:

*Dersom virksomheten ikke kan redusere sin avhengighet til en annen virksomhet, skal virksomheten sende en oversikt over hvilke virksomheter den er avhengig av for å fungere som den skal, jf. sikkerhetsloven § 4-2, til det departement som er ansvarlig for det forebyggende sikkerhetsarbeidet i sektoren, eller det departement som har fattet vedtak om at virksomheten skal omfattes av loven og Nasjonal sikkerhetsmyndighet.*

Ordlyden i dette forslaget bygger på høringsutkastets forslag til § 52, tredje ledd i virksomhetsforskriften som vi foreslår flyttet til § 11. NSM er av den oppfatning at bestemmelsen hører mer naturlig hjemme her da den er knyttet opp mot de risikovurderinger som skal gjøres etter lovens § 4-2, og da meldeplikten må anses hjemlet i denne bestemmelsen.

### Til § 16 Evaluering av produkt og tjeneste

Forslaget til bestemmelse legger til grunn at evalueringer og sertifiseringer skal utføres av NSM eller akkreditert laboratorium/sertifiseringsorgan utpekt av NSM. Vi mener det bør legges til rette for NSM også kan godkjenne produkter og tjenester evaluert og sertifisert i andre land. Bestemmelsen bør derfor endres slik at det fremgår at NSM, i sin sertifisering, kan legge til grunn sertifisering fra andre land.

NSM foreslår som nytt tredje ledd:

*Nasjonal sikkerhetsmyndighet kan godkjenne produkter evaluert og sertifisert i andre land til bruk etter § 15.*

### Til § 19 Unntak fra sikkerhetskrav

Myndigheten til å gi unntak fra sikkerhetskrav, som er hjemlet i loven § 5-2 og 6-2, er i forskriften foreslått lagt til NSM. NSM er imidlertid av den oppfatning at de ulike departementene må være involvert dersom unntak innvilges. Dette vil være mer i tråd med lovens intensjon om å tydeliggjøre sektoransvaret.

NSM foreslår som nytt siste ledd:

*Vedtaket skal fattes etter anmodning og uttalelse fra sektordepartementet.*

### Til § 21 Destruering av dokumenter og lagringsmedier med sikkerhetsgradert informasjon

NSM ser ikke behov for en godkjenningsordning på dette området. Veiledning fra NSM, samt krav til bruk av produkter som er evaluert og sertifisert etter § 16 framstår som mer hensiktsmessig enn godkjenningskravet i § 21.

NSM foreslår å stryke andre ledd.

### Til § 25 Kryptering

Etter andre ledd i forslaget skal virksomheten kryptere sikkerhetsgradert informasjon som er lagret hvis ikke informasjonen er sikret med andre sikkerhetstiltak. Begrepet «andre sikkerhetstiltak» er for vagt. Det bør stilles krav til at sikkerhetstiltakene må gi tilfredsstillende sikring av informasjonen i henhold til graderingsnivå.

NSM foreslår at andre ledd endres til:

*Sikkerhetsgradert informasjon som er lagret hos virksomheten, skal krypteres dersom informasjonen ikke er sikret med andre tilfredsstillende sikkerhetstiltak ut fra informasjonens graderingsnivå»*

### Til § 37 Kontrollert sone

I høringsnotatet heter det at § 37 *Kontrollert sone* i hovedsak er en videreføring av nåværende forskrift om informasjonssikkerhet § 6-7. NSM mener imidlertid det er vanskelig å lese ordlyden i § 37 som en videreføring av § 6-7. Formuleringen «personer og kjøretøy» i § 37 første ledd er vesentlig snevrere enn formuleringene «aktiviteten» i § 6-7 første ledd og «adgang og ferdsel» i begge paragrafers annet ledd. Innsnevringen er lite hensiktsmessig når formålet er effektiv kontroll. Den eksplisitte bortvisningsadgangen i § 6-7 første ledd er heller ikke videreført i § 37.

NSM foreslår at bestemmelsen endres til:

*En kontrollert sone skal være et tydelig avgrenset område der virksomheten kan kontrollere all aktivitet og bortvise uvedkommende.*
*Ved høy sikkerhetsrisiko skal adgang og ferdsel kontrolleres med en fysisk avgrensning.*

### Til § 38 Beskyttet sone

Etter forslagets andre ledd skal NSM godkjenne oppbevaringsenheter. NSM ser ikke behov for en slik godkjenningsordning. NSM mener at bestemmelsen bør endres slik at det stilles krav om bruk av oppbevaringsenhet som gir et «forsvarlig sikkerhetsnivå» for det aktuelle graderingsnivået. Dette vil gi virksomhetene en viss grad av fleksibilitet til og selv å vurdere hva som er forsvarlig nivå sett ut i fra egen risikovurdering. NSM vil også i sine veiledere kunne gi anbefalinger om hvordan forsvarlighetskravet kan tilfredsstilles.

NSM foreslår at andre ledd endres til:

*I beskyttet sone skal dokumenter og lagringsmedier med informasjon som er gradert KONFIDENSIELT eller høyere lagres i en oppbevaringsenhet som gir forsvarlig sikkerhet for det aktuelle graderingsnivået, eller oppbevares under permanent vakthold.»*

### Til § 39 Sperret sone

Paragrafen gir ikke bestemmelser om oppbevaring av sikkerhetsgradert informasjon i sperret sone. NSM mener at dette bør reguleres i et nytt ledd på tilsvarende måte som i § 38

NSM foreslår følgende nytt tredje ledd i § 39:

*I sperret sone skal dokumenter og lagringsmedier med informasjon som er gradert KONFIDENSIELT eller høyere lagres i en oppbevaringsenhet som gir forsvarlig sikkerhet for det aktuelle graderingsnivået, eller oppbevares under permanent vakthold.*

Nåværende tredje og fjerde ledd blir med denne endringen nytt fjerde og femte ledd.

### Til § 40 Behandling av informasjon gradert KONFIDENSIELT eller høyere

Forslaget til fjerde ledd innebærer at en virksomhet kan godkjenne at f.eks. et STRENGT HEMMELIG lagringsmedium kan medbringes på utenlandsreise såfremt «en person tar vare på» informasjonen gjennom hele reisen, det er mulig å deponere informasjonen ved en norsk utenriksstasjon, og reisen skjer til NATO land eller land Norge har sikkerhetsavtale med. I dag er dette bare mulig for informasjon gradert opp til KONFIDENSIELT. Lempingen på dette kravet er ikke gitt noen nærmere begrunnelse i høringsnotatet. NSM mener at det som en generell regel ikke er forsvarlig at informasjon gradert HEMMELIG og STRENGT HEMMELIG medbringes på reise utenlands. Dagens regulering bør videreføres. NSM ser imidlertid at enkelte virksomheter har behov for medbringelse av høyt gradert informasjon på reise på jevnlig basis. I disse tilfeller bør dette løses gjennom dispensasjonsbestemmelsen i forskriftens § 19 i form av generelle eller konkrete dispensasjoner.

### Til § 47 Godkjenningsmyndighet

NSM ser det som hensiktsmessig at saksbehandlingskapasitet i kompetente organisasjoner kan utnyttes som supplement til NSMs egen godkjenningskapasitet. Forslaget åpner imidlertid ikke for at NSM kan bemyndige andre til å godkjenne informasjonssystemer etter tredje ledd.

NSM foreslår derfor å tilføye et nytt femte ledd:

*Nasjonal sikkerhetsmyndighet kan gi fullmakt til andre organisasjoner til å godkjenne informasjonssystemer etter tredje ledd.*

## Til § 48 Godkjenningen

Departementet ber om innspill på om godkjenningsbestemmelsen er hensiktsmessig utformet.

Virksomhetsforskriften § 45 gir funksjonelle krav til sikring i skjermingsverdige informasjonssystemer, herunder funksjonelle krav til tiltak, og til utvelgelsen av tiltakene. Disse kravene er grunnlag for sikkerhetsgodkjenning jf. § 48. I tillegg stiller § 48 krav til den prosessen som må gjennomføres for å oppnå og vise samsvar med kravene i § 45.

Godkjenning, som et uttrykk for tillit, er følgelig både basert på vurdering av tiltak som er valgt i en gitt situasjon og på vurdering av prosessen som ligger til grunn for valgene. En slik vurdering av valg og grunnlag for valg gir større fleksibilitet i godkjenningsarbeidet. Tillit skapes av prosessen og ikke kun av et (statisk) utvalg tekniske tiltak. En slik tilnærming vil også lette arbeidet med regodkjenning etter endringer av eksempelvis kun deler av grunnlaget for den opprinnelige sikkerhetsgodkjenningen.

På denne bakgrunn er NSMs vurdering at forskriftens godkjenningsbestemmelser er hensiktsmessig utformet og i god sammenheng med kravene i § 45. Godkjenningsbestemmelsene slik den er foreslått vil gi grunnlag for en fleksibel, prosessrettet tilnærming for synliggjøring av tillit gjennom sikkerhetsgodkjenning.

Bestemmelsens innledning bør imidlertid klargjøres for å synliggjøre virksomheten som det primære pliktsubjekt:

*Godkjenningen skal baseres på en planlagt og systematisk gjennomgang for å oppnå et forsvarlig sikkerhetsnivå for informasjonssystemet. Virksomheten skal dokumentere at den på en tilfredsstillende måte har vurdert og håndtert risiko ved å ha:...:*

## Til § 52 Skadevurdering

Etter NSMs oppfatning vil virksomhetens skadevurdering være et premiss for departementenes utpeking og klassifisering av skjermingsverdig objekter og infrastruktur. Skadevurderingen må derfor knyttes opp mot lovens §§ 7-1 og 7-2.

Bestemmelsen er foreslått plassert under kapittel 7 «Beskyttelse av skjermingsverdige objekter og infrastruktur». Dette blir misvisende. Bestemmelsen bør tas inn i et kapittel som omhandler utpeking og klassifisering. Videre bør det tydeliggjøres at skadevurderingen ikke bare er et premiss for departementets klassifisering, men også for vedtaket om utpeking. Bestemmelsens ordlyd må justeres for å tilrettelegge for dette, og at skadevurderingen skal gjøres forut for departementenes utpeking. Tilsvarende må det også endres som nødvendig i myndighetsforskriften.

Bestemmelsen legger opp til at virksomheten selv skal vurdere objektets og infrastrukturens betydning for grunnleggende nasjonale funksjoner. Det tilligger departementene å vurdere hvilken betydning et objekt eller en infrastruktur har for grunnleggende nasjonale funksjoner. Virksomheten vil heller ikke ha tilstrekkelig oversikt for å kunne vurdere dette fullt ut. De enkelte departementer vil derfor måtte gjøre en bredere vurdering basert på innspill fra virksomheter i sin sektor, samt på andre tilgjengelige informasjonskilder.

Videre foreslår NSM å stryke § 52 tredje ledd og flyttet dette til § 11.

### Til § 57 Virksomhetens rett til innsyn

Når det gjelder virksomhetens rett til innsyn i VDI konfigurasjoner så støtter NSM bestemmelsen i sitt hovedtrekk, men påpeker at dette må gjelde ugraderte signaturer. Der hvor det benyttes en gradert signatur må dette reguleres etter reglene for gradert informasjon. For øvrig påpekes, i tilknytning til bestemmelsens siste punktum, at data som NSM mottar fra virksomheten, eies av virksomheten. En regulering av innsynsrett for virksomheten til disse dataene kan bidra til å skape usikkerhet til eierskapet til dataene, da det gir inntrykk av at NSM eier dataene.

### Til § 58 Vilkår for å gi autorisasjon

Forslaget til bestemmelse viderefører ikke alle autorisasjonskriteriene som følger av dagens § 5-2. Slik vi forstår høringsnotatet er det ikke ment å gjøre materielle endringer i forhold til dagens autorisasjonsregime. Av hensyn til klarhet mener vi derfor at dagens kriterier bør videreføres samlet i § 58.

### Til § 62 Nødautorisasjon

Forslaget til ny bestemmelse knytter nødautorisasjon opp mot *nødrett* etter straffeloven. I dag er det lagt til grunn at nødautorisasjon også kan benyttes der det er nødvendig ut fra *tvingende beredskapsmessige hensyn* eller *operative forhold.* Det kan synes som at terskelen for å nødautorisere med dette heves slik at eksempelvis beredskapshensyn ikke omfattes. NSM legger til grunn at dette ikke er hensikten.

Gjeldende krav om lavere klarering for å kunne nødautoriseres for STRENGT HEMMELIG (SH)/ COSMIC TOP SECRET (CTS)er ikke videreført. NSM mener at man ved nødautorisasjon for SH/CTS i en beredskapssituasjon vil løpe en betydelig risiko for at det oppstår avgjørende skadefølger for nasjonale sikkerhetsinteresser dersom man ikke krever en viss bakgrunnskontroll. NSM mener derfor at bestemmelsen om nødautorisasjon i større grad bør formuleres i tråd med gjeldende forskrift om personellsikkerhet § 5-3. Dersom det er behov for å gi en person uten noen form for sikkerhetsklarering tilgang til skjermingsverdig informasjon, objekt eller infrastruktur for å avverge direkte fare for liv og helse, vil dette uansett kunne gjøres innenfor rammen av straffelovens § 17.

NSM foreslår at § 62 endres til:

*I nødsituasjoner kan en person autoriseres uten å inneha nødvendig sikkerhetsklarering, dersom det ikke foreligger rimelig tvil om vedkommendes pålitelighet, lojalitet eller sunne dømmekraft.*

*Nødautorisasjon for STRENGT HEMMELIG (eventuelt COSMIC TOP SECRET/tilsvarende) kan bare gis til personer som innehar gyldig sikkerhetsklarering for en lavere sikkerhetsgrad, med mindre NSM gir dispensasjon i hvert enkelte tilfelle.*

*Virksomheten skal uten ugrunnet opphold varsle Nasjonal sikkerhetsmyndighet om hvilke personer som har nødautorisasjon og på hvilket nivå.*

### Til § 64 Dokumentasjon på autorisasjon

Dokumentasjonen bør også inneholde eventuelle vilkår eller avgrensinger knyttet til autorisasjonen, og NSM foreslår at dette tas inn i bestemmelsen. Dette er nødvendig for å ivareta formålet med å fastsette vilkår etter lov om nasjonal sikkerhet § 8-6.

### Til § 66 Begrunnelse og dokumentasjon ved forespørsel om klarering

Slik NSM ser det, medfører høringsnotatets tolkning av kravet til dokumentasjon et vesentlig svakere grunnlag for klareringsmyndighetene til å vurdere om det foreligger et reelt klareringsbehov. Ansvaret for å dokumentere behovet i det enkelte tilfellet overføres nå i praksis til klareringsmyndighetene. Henvisningsteknikken vil åpne for mindre presisjon i begrunnelsene, og påføre klareringsmyndighetene merarbeid knyttet til å dokumentere det faktiske behovet i den enkelte sak. NSM legger til grunn at dersom tolkningen av bestemmelsen som kommer til uttrykk i høringsnotatet legges til grunn for praktiseringen av bestemmelsen, vil dette føre til en svakere kontroll med anvendelsen av klareringsinstituttet enn hva gjelder i dag, samt en økt risiko for at det gjennomføres personkontroller uten at det foreligger et reelt behov for sikkerhetsklarering.

### Forslag til nye bestemmelser i virksomhetsforskriften kapittel 9:

For at klareringsmyndighetene skal kunne foreta konkrete og individuelle vurderinger knyttet hensiktsmessighet og bruk av vilkår og stillingsklarering, er det nødvendig å ha et tilstrekkelig informasjonsgrunnlag. I denne sammenheng vil det særlig være behov for å innhente informasjon om forhold knyttet til arbeidsoppgaver, arbeidssted og risikovurderinger foretatt av virksomheten hvor vedkommende skal autoriseres. NSM mener på denne bakgrunn at det er behov for å etablere en tydelig plikt for virksomhetene til å gi den informasjonen som er nødvendig når det anmodes om klarering, samt en plikt til å følge opp gitte vilkår.

NSM foreslår på denne bakgrunn to nye bestemmelser i virksomhetsforskriftens kapittel 9:

*§ X Autorisasjonsansvarliges plikt til å utlevere informasjon til klareringsmyndigheten*

*Virksomheten skal etter anmodning, eller når virksomheten finner grunn til det, gi de opplysninger som er nødvendig for at klareringsmyndigheten skal kunne vurdere vilkår etter sikkerhetsloven § 8-6. Informasjonsplikten gjelder i hele autorisasjonsperioden.*
*Plikten til å utlevere opplysninger etter denne bestemmelsen gjelder uten hinder av taushetsplikt.*

*§ X Autorisasjonsansvarliges plikt til å legge til rette for og oppfylle vilkår knyttet til klarering*

*Autorisasjonsansvarlig skal legge til rette for og oppfylle de vilkår som stilles av klareringsmyndigheten i forbindelse med vedtak om klarering. Dersom gitte vilkår ikke lar seg oppfylle, skal autorisasjonsansvarlig orientere klareringsmyndigheten om dette så snart det er mulig. Autorisasjonen skal i tillegg vurderes i samsvar med sikkerhetsloven § 8-10.*

### Særskilt om informasjons- og informasjonssystemsikkerhet

Virksomhetssikkerhetsforskriften gir bestemmelser for hva som skal til for å oppnå et forsvarlig sikkerhetsnivå for beskyttelse av skjermingsverdig informasjon, informasjonssystemer samt infrastruktur og objekt. For å oppnå et forsvarlig sikkerhetsnivå må disse leses i sammenheng. NSM støtter forskriftenes innretning om et klarere skille mellom høygradet og annen skjermingsverdig informasjon.

Men NSM mener det er behov for en harmonisering av ordlyd og begrepsbruk for å synliggjøre sammenhengen mellom de ulike nivåene på skjermingsverdig informasjon og en større tydelighet på hvordan de ulike bestemmelsene henger sammen. Det er i forarbeidene skrevet at sikkerhetsgradert informasjon skal ha «*enhetlig og helhetlig [beskyttelse] på tvers*

*av alle sektorer*, for å oppnå dette er det nødvendig å ha bestemmelser som gjør det lettere å se sammenhengen mellom de ulike nivåene.

Bestemmelsene i §§ 20 og 32 definerer hva som er et forsvarlig sikkerhetsnivå for behandling av informasjon. Men bestemmelsene bygger på to ulike tilnærmingsmåter.

For BEGRENSET og skjermingsverdig informasjon er forsvarlig sikkerhetsnivå oppfylt dersom informasjonen ikke med enkle midler kan endres, gå tapt eller gjøres utilgjengelig. Bestemmelsen bygger med andre ord på trussel aktørens kompetansenivå. § 32 bygger imidlertid på at virksomheten skal oppnå definerte sikkerhetsmål for å oppnå forsvarlig sikkerhet. Dette gjør at ordlyden i bestemmelsene §§ 20 og 32 ikke får en naturlig sammenheng. NSM mener det er hensiktsmessig at disse to bestemmelsene benytter lik ordlyd og metodikk. Vi mener videre at §§ 20 og 32 bør rendyrke et konfidensialitetshensyn da dette er dette er hensynet bak gradering av informasjon. Integritets og tilgjengelighetsprinsippene reflekteres mer naturlig i § 45.

På STRENGT HEMMELIG nivå oppstiller forskriftens § 32 et absolutt krav til sikring. Risiko vil aldri kunne minimeres fullstendig, og NSM foreslår derfor at det stilles et noe mer reelt sikringsmål for dette graderingsnivået.

Basert på dette foreslår NSM følgende ordlyd i §§ 20 og 32:

*§ 20 Forsvarlig sikkerhetsnivå for skjermingsverdig informasjon*

*Når virksomheten håndterer risikoen knyttet til skjermingsverdig informasjon, jf. § 12, er kravet til et forsvarlig sikkerhetsnivå oppfylt dersom virksomheten har etablert risikoreduserende tiltak for å hindre at personer kan få uønsket tilgang til informasjonen.*

*Risikoreduserende tiltak for informasjonssystemer skal være i samsvar med § 45.*

*For informasjon som er gradert KONFIDENSIELT eller høyere, gjelder i tillegg reglene i Kapittel 5.*

*§ 32 Forsvarlig sikkerhetsnivå for informasjon gradert KONFIDENSIELT eller høyere*

*Når virksomheten håndterer risikoen knyttet til sikkerhetsgradert informasjon, jf. § 12, er kravet til et forsvarlig sikkerhetsnivå oppfylt dersom*

*a) personer ikke kan få uønsket tilgang til informasjon gradert KONFIDENSIELT eller høyere uten at virksomheten oppdager og kan begrense skadefølgene*
*b) personer ikke kan få uønsket tilgang til informasjon gradert HEMMELIG eller høyere uten at virksomheten oppdager det i tide til å kunne motvirke kompromittering og kan begrense skadefølgene*
*c) personer ikke kan få uønsket tilgang til informasjon gradert STRENGT HEMMELIG uten at virksomheten oppdager dette umiddelbart og kan hindre skadefølger.*

*For informasjonssystemer beskrives forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer i § 45.*

NSM vil påpeke at Norge har en forpliktelse til å beskytte informasjon mottatt fra NATO og andre internasjonale organisasjoner og land, i henhold til gitte standarder. For virksomheter som skal behandle sikkerhetsgradert informasjon mottatt fra annen stat eller internasjonal organisasjon må §§ 20 og 32 fortolkes i lys av våre internasjonale forpliktelser.

Virksomhetsforskriftens § 45 gir bestemmelser om beskyttelse av skjermingsverdige informasjonssystemer. Bestemmelsen må leses i sammenheng med §§ 20 og 32 da

virksomheten må implementere tiltakene ulikt avhengig av hvilen informasjon som skal behandles i systemet, og informasjonens eventuelle graderingsnivå. Dette kommer i liten grad frem og bør synliggjøres i bestemmelsen. Videre bør det tas inn i § 45 at for informasjonssystemer som klassifiseres som skjermingsverdig infrastruktur eller objekt så får § 53 anvendelse i tillegg til § 45, jf. §§ 20 og 32. Videre bør § 53 synliggjøre forholdet mellom de ulike bestemmelsene i sin ordlyd.

For å synliggjøre dette foreslår NSM et nytt siste ledd i § 45:

*Behovet for å beskytte både konfidensialitet, integritet og tilgjengelighet må ses i sammenheng og avveis mot hverandre. Kravene i denne bestemmelsen må også sees i sammenheng med forskriftens kapittel 2 og §§ 20, 32 og 53.*

## 2.3 Merknader til forskrift om klarering av leverandører og personell. (klareringsforskriften)

### Til § 1 Klareringsmyndighet

Departementet ber om høringsinstansenes syn på fjerde ledd i bestemmelsen som stiller krav om at personell som utøver klareringsmyndighet skal ha klarering for det høyeste klareringsnivå som personellet er gitt myndighet til å fastsette. NSM støtter forslaget

Det bør tas inn et krav om at ansatt ved klareringsmyndighet kun kan inneha norsk statsborgerskap. Personellsikkerhetsregelverket legger opp til at det skal tas særskilte sikkerhetsmessige hensyn ved vurdering av utenlandske statsborgeres mulighet til å få tilgang til skjermingsverdig informasjon, objekter og infrastruktur. Vurderingene er i stor grad skjønnsmessige, og den enkelte saksbehandler ved klareringsmyndighetene vil kunne ha betydelig påvirkning på utfallet av en klareringssak. Det er NSMs oppfatning at dette gjør klareringsmyndighetene til et mål for infiltrasjon. Ansettelse av utenlandske statsborgere i slike stillinger øker risikoen for dette, samtidig som skadepotensialet er stort. Grunnleggende sikkerhetshensyn tilsier derfor at utenlandske statsborgere ikke bør foreta disse vurderingene.

NSM foreslår som et nytt femte ledd:

*Personell som forbereder eller avgjør klareringssaker kan ikke inneha andre statsborgerskap enn norsk.*

### §2 Definisjoner

NSM mener opplistingen i bokstav b, «nær familie» kan kortes ned, da det er flere av de opplistede kategoriene som kan oppleves som for fjern tilknytning til at det skal regnes som nær familie. NSM foreslår at punkt 2 og 4 under bokstav b) slettes.

Videre mener NSM at avgrensningen i bokstav d «annen nær tilknytning» er for snever, og antakelig ikke i samsvar med forarbeidene til lov om nasjonal sikkerhet. Det avgjørende må være om personen kan påvirke hovedpersonens sikkerhetsmessige skikkethet. Det må være opp til klareringsmyndigheten i det enkelte tilfelle å foreta denne vurderingen uavhengig av hvilken form den nære tilknytningen tar.

NSM foreslår at bokstav d skal lyde:

*d) annen nær tilknytning: en personlig relasjon som er av en slik art at personen kan påvirke vedkommendes sikkerhetsmessige skikkethet.*

**§ 7. Sikkerhetsklarering – krav til egenopplysninger**

NSM er enig i at det bør være en forutsigbarhet knyttet til hvilke egenopplysninger som kreves gitt i forbindelse med sikkerhetsklarering. Vi mener imidlertid at dette ikke bør detaljreguleres i forskrift fordi det gir for liten fleksibilitet i forhold til samfunnsutviklingen. NSM ønsker å påpeke at en må legge til rette for digitalisering, og derfor gi en viss fleksibilitet knyttet til hvilke opplysninger som skal gis av den klarerte og hvilke som kan hentes direkte fra ulike offentlige registre. NSM ønsker derfor at ordet «skjema» ikke benyttes i forskriftsteksten.

En opplisting i forskriften av hva det skal opplyses om, vil kunne få konsekvenser i form av utilsiktede avgrensninger av tema. Den foreslåtte bestemmelsens første ledd bokstav i, k, n og o inneholder slike avgrensinger. Bestemmelsen legger videre opp til at hovedpersonen selv skal vurdere relevansen av forhold som det skal opplyses om. NSM kan ikke se at dette har vært lovgivers intensjon.

Behovet for å kunne gi pålegg om å gi relevante opplysninger til klareringsmyndigheten bør etter NSMs oppfatning kunne ivaretas tilstrekkelig gjennom en enkelt setning, som eksempelvis "...gi opplysninger som *er nødvendig for å gjennomføre personkontroll og ta stilling til vedkommendes sikkerhetsmessige skikkethet etter sikkerhetsloven § 8-4.*".

Behovet for forutsigbarhet for den enkelte bør kunne ivaretas ved en publisert oversikt over de egenopplysninger som til enhver tid kreves av den enkelte, eksempelvis på NSMs hjemmeside. NSM gjør oppmerksom på at personopplysningsblanketten også i dag er et offentlig tilgjengelig dokument, og at den kun benyttes etter samtykke fra den enkelte.

NSM foreslår at § 7 endres til:

*Den som skal sikkerhets- eller adgangsklareres gi opplysninger som er nødvendig for at klareringsmyndigheten skal kunne be om personkontroll og ta stilling til vedkommendes sikkerhetsmessige skikkethet etter sikkerhetsloven § 8-4.*

NSM vi også gjøre oppmerksom på at departementets forslag til første og andre ledd avgrenser hvilke nærstående det skal gis informasjon om på de ulike klareringsnivåene. På denne måten hindres klareringsmyndigheten i praksis i å foreta vurderingen av hvilke nærstående som skal omfattes av personkontrollen etter § 6 andre ledd. Eksempelvis vil nåværende og tidligere statsborgerskap for andre nærstående enn de som nevnes i § 7 andre ledd særlig være relevant i vurderingen etter § 6 andre ledd.

For det tilfelle at det blir valgt å beholde en opplisting av krav til egenopplysninger foreslår NSM følgende ny ordlyd innledningsvis i § 7, første ledd:

*Den som skal sikkerhetsklareres for KONFIDENSIELT skal gi sitt samtykke til gjennomføring av personkontroll. I den forbindelse kan NSM stille spørsmål om…*

*Videre foreslår vi at andre og tredje ledd endres til:*

*Ved en sikkerhetsklarering for HEMMELIG, NATO SECRET eller tilsvarende kan NSM be om opplysninger angitt i a-c om nåværende ektefelle, partner eller samboere.*

*Ved en sikkerhetsklarering for STRENGT HEMMELIG, COSMIC TOP SECRET eller tilsvarende kan NSM, i tillegg til opplysninger nevnt i foregående ledd, be om opplysninger tilsvarende opplysninger for øvrige personer nevnt i § 2, bokstav b).*

NSM mener også at opplistingen må endres slik at den som gir opplysninger ikke selv skal foreta vurderinger som etter lovens § 8-4 tilligger klareringsmyndigheten. Dette gjelder bokstavene i, k, n og o.

NSM vil videre bemerke at det i høringsnotatet pkt. 8.2.3 siste avsnitt uttales at det ikke er nødvendig å gi fullstendige opplysninger om alle temaene som er listet opp i § 7. NSM mener at formuleringen er uheldig, idet det kan gi den som skal gi opplysningene et inntrykk av at vedkommende selv kan velge hvor fullstendig opplysninger vedkommende skal gi. Det må være opp til sikkerhetsmyndigheten å angi hvilket presisjonsnivå det skal være på de forskjellige opplysningene.

### § 8. Adgangsklarering – krav til egenopplysninger

NSM viser til merknadene til kapittel 7, og legger disse til grunn også i forhold til § 8.

NSM gjør oppmerksom på at departementets forslag til bestemmelse medfører at klareringsmyndighetene ikke vil få opplysninger om *tilknytning til andre stater* for nivået adgangsklarering, noe som kan være relevant ved vurdering knyttet opp mot hensikten - forebygging av terror. Bestemmelsen vil videre føre til at norske myndigheter ikke vil ha oversikt over utenlandske borgere med adgang til skjermingsverdige objekter eller infrastruktur. Manglende egenopplysninger om statsborgerskap vil videre være til hinder for oppfyllelse av NSMs plikt til å gi informasjon til Politiets sikkerhetstjeneste etter lov om nasjonal sikkerhet § 8-12.

### § 14. Personhistorikk

NSM mener at flere av unntakene som listes i bestemmelsens fjerde ledd, trekker oppmerksomheten vekk fra det som er vesentlig når det gjelder formålet med et krav om personhistorikk, nemlig å opplyse saken på en slik måte at det er mulig å ha en *kvalifisert oppfatning* av om en person kan anses sikkerhetsmessig skikket til å inneha en klarering. I vurderingen av hvilken betydning manglende personhistorikk skal ha i skikkethetsvurderingen, er det mange forhold som vil inngå. NSM mener derfor at det er en risiko for at vurderingen blir for sjablonmessig ved å peke på enkelte av disse forholdene. NSM mener derfor at fjerde ledd bør forenkles og gjøre mer generell.

NSM foreslår § 14 fjerde ledd endres til:

*Etter en konkret helhetsvurdering kan klarering likevel gis selv om kravet til personhistorikk i første til tredje ledd ikke er oppfylt. I vurderingen skal det blant annet legges vekt på om mangelen på personhistorikk er av liten betydning for vurderingen av personens sikkerhetsmessige skikket. Videre kan det legges vekt på om det foreligger tilgang til personhistorikk utover de siste 10 år som kan avbøte for manglende personhistorikk de siste 10 år.*

## § 15 Vurderingsgrunnlaget for adgangsklarering

NSM mener at vurderingsgrunnlaget for adgangsklarering ikke bør angis som et utvalg av forhold etter lovens § 8-4 fjerde ledd. Det vesentlige er at vedkommende som vurderes klarert, kun kan gis klarering dersom vedkommende er *sikkerhetsmessig skikket.* NSM mener at det er tvilsomt om klareringsmyndigheten kan anse en person som sikkerhetsmessig skikket etter lovens § 8-4, dersom det på grunn av forhold som ikke omfattes av forslaget til bestemmelse, er rimelig tvil om skikketheten.

NSM mener at formålet med de ulike nivåer av adgangsklarering, sammenholdt med det informasjonstilfanget som forutsettes i § 10, i tilstrekkelig grad vil sette rammene for hvilken risiko klareringsmyndighetene bør akseptere på de ulike nivåene. Siden formål og risikoaksept knyttet til adgangsklarering ikke kan utledes av lovens § 8-4, mener NSM likevel at det bør inntas en overordnet bestemmelse om dette i forskriften.

NSM foreslår § 15 skal lyde:

*I vurderingen av sikkerhetsmessig skikkethet for adgangsklarering etter sikkerhetsloven § 8-4 skal det i hovedsak legges vekt på forhold som er relevant for planlegging, gjennomføring eller forsøk på terror.*

*I vurderingen av sikkerhetsmessig skikkethet for utvidet adgangsklarering etter sikkerhetsloven § 8-4 skal det i tillegg til terrortrusselen legges vekt på forhold som er relevant for planlegging, gjennomføring eller forsøk på spionasje, sabotasje, attentat eller liknende.*

## § 16 Vurderingsgrunnlaget for tilknytning til andre stater

Departementet ber om høringsinstansenes syn på bestemmelsen, herunder om momentene i tilknytningsvurderingen bør fremgå tydeligere av forskriftene.

Lov om nasjonal sikkerhet § 8-4 fjerde ledd bokstav n) *tilknytning til andre stater* og § 8-7 *hjemlandets sikkerhetsmessige betydning* setter rammene for temaet. NSM mener at den foreslåtte ordlyden til § 16 virker avgrensende hva gjelder vurderingskriterier ved tilknytning til andre stater, og kan ikke se at dette har vært forutsatt i forarbeidene til sikkerhetsloven. Tilknytning til andre stater kan ha en mangeartet form. Hvilke momenter som kan få betydning for vurderingen av sikkerhetsmessig skikkethet vil være individuelle og påvirkes av bl.a. landets sikkerhetsmessige betydning og den aktuelle sikkerhetspolitiske situasjon. Også ikke-statlige aktører vil kunne ha evne og vilje til å påvirke vedkommendes skikkethet. NSM mener derfor at momentene i tilknytningsvurderingen ikke kan reguleres i forskriften. Når det gjelder graden av sikkerhetssamarbeid mellom Norge og den andre staten, vil dette være en del av vurderingen av landets sikkerhetsmessige betydning. Det er derfor ikke nødvendig å nevne dette elementet av vurderingen spesielt i bestemmelsen.

NSM foreslår at § 16 skal lyde:

*I vurderingen av tilknytning til andre stater etter sikkerhetsloven § 8-4 fjerde ledd bokstav n, skal klareringsmyndigheten legge vekt på Nasjonal sikkerhetsmyndighets vurdering av statens sikkerhetsmessige betydning.*

## § 17 Klareringsintervju

NSM mener det er uheldig å innføre et nytt begrep for disse samtalene. Man innfører så fall en tredje type samtale innenfor personellsikkerhetsregelverket i tillegg til *sikkerhetssamtale* og *autorisasjonssamtale*. NSM er i tvil om dette vil ivareta de pedagogiske hensyn som synes å begrunne forslaget. Sikkerhetssamtale er et godt innarbeidet begrep som også benyttes i lov om nasjonal sikkerhet. Med den etablerte metodikken som klareringsmyndighetene benytter, er det heller ikke naturlig å omtale disse samtalene som et intervju.

Bestemmelsens andre ledd er nytt, og har en ordlyd som tilsynelatende setter begrensinger for hva som kan være tema i en sikkerhetssamtale. NSM kan ikke se at lov om nasjonal sikkerhet eller forarbeidene til denne legger opp til en avgrensning av hvilke opplysninger som kan innhentes i en sikkerhetssamtale. Hensikten er tvert imot, slik NSM ser det, at klareringssaken skal kunne opplyses så godt som mulig. NSM mener at referansen til sikkerhetsloven § 8-4 fjerde ledd er for snever, idet sikkerhetssamtalen også må kunne benyttes til å innhente opplysninger som er relevante for å vurdere saken etter øvrige ledd i paragrafen, §§ 8-6, 8-7, 8-8, 8-9, samt en rekke bestemmelser i forskrift om klarering av leverandører og personell. Høringsnotatet pkt. 8.3.3 tredje avsnitt modererer for så vidt begrensingene i ordlyden ved å fastslå at «*Rammen skal ikke forhindre deltakerne i intervjuet å snakke om øvrige forhold, men dette faller da utenfor vurderingen klareringsmyndigheten gjør i etterkant av intervjuet.*» NSM mener at rammen for hvilke forhold som kan inngå i vurderingen av sikkerhetsmessig skikkethet, er gitt i lov om nasjonal sikkerhet § 8-4, og at det dermed ikke er nødvendig å gjenta dette i forskriften. For å unngå uklarhet bør annet ledd omformuleres.

NSM foreslår at § 17 andre ledd skal lyde:

*Formålet med sikkerhetssamtale er å innhente opplysninger som er relevante for å kunne vurdere sikkerhetsmessig skikkethet etter sikkerhetsloven kapittel 8 og denne forskrift.*

## Til kapittel 4 Samtykke til å autorisere utenlandske statsborgere for BEGRENSET

Departementet ber om høringsinstansenes innspill knyttet til hensiktsmessigheten av bestemmelsene i kapittel 4. NSM mener det er behov både for å ha en to-nivå avgjørelse knyttet til autorisasjon av utenlandske statsborgere, og for å holde en løpende oversikt over utenlandsk personell som er autorisert for norsk informasjon. Dette bør reguleres i forskrift, og NSM støtter derfor de foreslåtte bestemmelsene i kapittel 4.

## Til § 29 Klareringsmyndighet for leverandørklarering

Vi støtter bestemmelsen om at NSM er klareringsmyndighet for norske leverandører i forbindelse med sikkerhetsgraderte anskaffelser. NSM utøver denne funksjonen i dag, og det er sentralt at den opprettholdes.

## Til § 32 Kilder for leverandørkontroll

NSM er enig i behovet for å tydeliggjøre kildene for leverandørkontroll, og mener at det er av viktighet at bestemmelsen blir stående i henhold til utkastets ordlyd.

## Forslag til ny bestemmelse:

### Omgjøring av klareringsavgjørelse til ugunst for den klarerte

Departementene og klagemyndigheten (NSM) har i gjeldende forskrift om personellsikkerhet § 4-1 hjemmel til å omgjøre en klareringsavgjørelse til ugunst for den klarerte dersom hensynet til rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser tilsier det. Dette er en hjemmel som er særlig praktisk for effektivt å regulere tilgang til sikkerhetsgradert informasjon, objekter og infrastruktur i en beredskapssituasjon.

Hjemmelen er ikke videreført i forslaget til ny forskrift. NSM kan etter dette ikke lenger suspendere eller trekke tilbake en gitt sikkerhets- eller adgangsklarering for enkeltpersoner eller grupper dersom sikkerhetssituasjonen skulle tilsi det. Dette fører til en betydelig økt risiko for innsidevirksomhet i en krise eller konfliktsituasjon.

NSM foreslår at hjemmelen videreføres i klareringsforskriften kapittel 3, eventuelt i myndighetsforskriften:

*§ X Omgjøring av klareringsavgjørelse uten klage*

*Dersom hensynet til nasjonale sikkerhetsinteresser tilsier det, kan klageinstansen eller overordnet departement omgjøre en klareringsavgjørelse til skade for den som avgjørelsen retter seg mot. Forvaltningsloven § 35 gjelder ikke.»*

Kjetil Nilsen
Direktør

*Dette dokumentet er elektronisk godkjent hos Nasjonal sikkerhetsmyndighet og sendes uten signatur.*

Kopi til:

Justis- og beredskapsdepartementet, Postboks 8005 Dep, 0030 OSLO, Norge