FFI Forsvarets forskningsinstitutt

Dato:	Vår referanse:	Deres referanse:
3. oktober 2018	17/16868-5 / 016	2015/3139-254

Forsvarsdepartementet

Postboks 8126, Dep
0032 OSLO

Høring - Forskrifter til ny sikkerhetslov

FFI viser til høringsbrev mottatt fra FD 2/7 2018. FFIs høringsinnspill gir innledningsvis noen overordnede kommentarer. Deretter følger detaljerte innspill til enkeltparagrafer i de tre forskriftene. Det vil ikke bli gitt innspill til kommentarene på forskriftsutkastet, men svar på de fleste konkrete spørsmålene er gitt som vedlegg.

Overordnede kommentarer

Etter FFIs vurdering utgjør lov om nasjonal sikkerhet (sikkerhetsloven) et godt grunnlag for forebyggende sikkerhet de nærmeste årene. I lys av en rivende teknologisk utvikling er det imidlertid viktig fortløpende å følge opp at loven også over tid følger behovene gitt av samfunnsutviklingen. Etter FFIs syn er forslaget til forskrifter i hovedsak et godt verktøy for å etablere et nytt regime under den nye loven.

FFI er av den oppfatning at forskriftene gjennom manglende balanse i forskriftsbestemmelsene, i for stor grad reflekterer dagens sikkerhetsregime, og ikke i tilstrekkelig grad tar i bruk de mekanismer som ligger til grunn i den nye loven. Etter FFIs syn bør dette være en lov med fokus på hensynet til nasjonal sikkerhet og statssikkerhet. Dette bør begrenses til sikkerhet mot tilsiktede handlinger i den øvre del av krisespekteret; terror, hybride trusler, sikkerhetspolitiske kriser og væpnet konflikt. Det bør utvises forsiktighet med bestemmelser som kan oppfattes å utvide formålet til å omfatte dagligdagse hendelser og samfunnssikkerhet generelt. Det bør etter FFIs vurdering derfor gjøres en grundig gjennomgang av forskriftsforslaget for å kvalitetssikre at virkeområdet gitt av loven reflekteres i forskriftene. Særlig bør det sikres at Forsvarets interesser ved utvikling av effektivt militært materiell og effektive konsepter for kommando- og kontroll ivaretas spesielt.

Det framkommer også et inntrykk av at det i forskriftsforslaget legges stor vekt på tradisjonell sikring av objekter og informasjon, til tross for at det i loven prinsipielt legges vekt på sikring av grunnleggende nasjonale funksjoner (GNF). Det oppstår dermed en utydelighet som kan medføre

Vedlegg: 1

Saksbehandler:	Postboks 25, 2027 Kjeller	Sentralbord:	63 80 70 00		
Monica Endregard	Besøksadresse:	Dir:		Org.nr:	NO 970 963 340 MVA
monica.endregard@ffi.no	Instituttveien 20, 2007 Kjeller	Faks:	63 80 71 15	E-post:	ffi@ffi.no

utilsiktet uheldig forvaltning av lov og forskrift. En slik utydelighet er etter FFIs syn alvorlig og det bør gjøres en gjennomgang av forskriftene for å skape tydelighet og konsistens mellom de to sikkerhetsprinsippene.

Én årsak til at FFI ser et behov for kvalitetssikring av forskriftsforslagets bestemmelser om virkeområdet er at forskriftene potensielt også vil favne svært mange private virksomheter innen ulike former for vareleveranser og tjenester, som for eksempel infrastrukturer. Det er viktig at forskriftene ikke får unødvendig negativ utilsiktet innvirkning på norske eller utenlandske virksomheters konkurranseevne. En slik negativ innvirkning vil på sikt kunne medføre svakere tjenester, som igjen vil kunne gi svakere nasjonal sikkerhet.

Videre oppfattes virkeområdet og ansvarsfordeling mellom de ulike nivåene som noe uklart. Det kan framstå som at mange saker og vurderinger tilfaller både departements- og virksomhetsnivået, og det ser ut til at ansvaret veksler mellom de ulike nivåene før det tas en beslutning om f.eks. klassifisering. Av praktiske hensyn, og for de som skal gjennomføre f. eks. en skadevurdering, kan det være hensiktsmessig å vite hva som skal skje før en slik vurdering (bakgrunnen) og hva som skal skje etter at virksomhetene har gjennomført sin del (utfallet og bestemmelsene fra departementsnivået). FFI mener derfor at det bør vurderes om det innledningsvis i hver av de tre forskriftene bør redegjøres for hva som er formålet, hvordan gangen i prosessene er og hva sluttresultatet skal være.

I lovproposisjonen ble det lagt betydelig vekt på å utvide bestemmelsene om informasjonssikkerhet og informasjonssystemsikkerhet til også å omfatte hensynet til informasjonens tilgjengelighet og integritet. Dette ble gjort med særlig hensyn til behovet for robust evne til nasjonal krisehåndtering og Forsvarets evne til å gjennomføre militære operasjoner i krise og krig. Dette er i prinsippet ivaretatt i forskriftene, men forskriftene har også en betydelig vektlegging på tradisjonell konfidensialitetssikkerhet. Det er viktig at balansen mellom de ulike sikkerhetsegenskapene som blir innført i den nye loven ivaretas spesielt i den videre utviklingen av regimet.

Verken loven eller forskriftsforslaget ivaretar etter FFIs syn behovet for sikkerhet innen objekter og infrastrukturer. Som FFI oppfatter av høringsbrevet, ser også FD at bestemmelsene ikke har tilstrekkelig kvalitet. I høringsbrevet foreslår FD dette løst ved å videreføre dagens regime innen objektsikkerhet og så innarbeide bedre bestemmelser innen infrastruktursikkerhet gjennom det videre sikkerhetsarbeidet etter lovens ikrafttredelse. FFI ser at det er nødvending å videreføre dagens regime innen objektsikkerhet inntil det foreligger hensiktsmessige bestemmelser også om infrastruktursikkerhet. FFI er uenig i en tilnærming der bestemmelser om infrastruktursikkerhet skal utvikles over tid. FFI har erfaring fra en rekke analyser på sikkerhet innen flere typer sivile og militære infrastrukturer. Basert på dette arbeidet er det FFIs syn at objekt- og infrastruktursikkerhet er et svært omfattende og sammensatt område som krever en helhetlig tilnærming. Dette omfatter også stort behov for kunnskap fra ulike typer sektorer, i stor grad også private virksomheter. Det er høy risiko for at feil innretning på bestemmelsene vil kunne virke mot sin hensikt. Dette vil også kunne ha betydelige uheldige konsekvenser for mange av de private virksomhetene, som i dag står for både utvikling og drift av infrastruktur i Norge. FFI minner også om at Sikkerhetsutvalget la betydelig vekt på behovet for modernisering av dagens objektsikkerhetsregime til også å omfatte infrastrukturer. Det er svært bra at både loven og forskriftsforslaget legger til grunn en funksjonsinnretning for sikkerhet. Etter FFIs syn er dette imidlertid en svært krevende endring som vil fordre omfattende metodekunnskap i kombinasjon med kunnskap om de mange ulike funksjonene som nå potensielt kommer inn under loven. Det vil her være av stor betydning at behovet for slik kunnskap ivaretas på en tilstrekkelig god måte ved utvikling av regimet. En funksjonsinnretning krever god vurderingskompetanse. Det blir videre et større krav til styringssystemer for blant annet å kartlegge og vurdere risiko, og videre iverksette tilstrekkelige tiltak for å ivareta et forsvarlig sikkerhetsnivå. Samtidig, bør det etter FFIs syn, legges betydelig vekt på å utvikle nære relasjoner mellom ulike deler av forvaltningen og private virksomheter. FFI anbefaler at det vurderes å etablere tverrsektorielle scenarioer som grunnlag for risikovurderinger.

Forskriftene beskriver balansering av tiltak som nødvendig, men bør i større grad kreve balansert tverrsektoriell koordinering og styring ved valg av skjermingsverdige systemer, infrastrukturer og objekter, klassifisering av disse og håndtering av tiltak. Videre bør forskriftene presisere at redundans i seg selv er et sikringstiltak. Det er FFIs klare oppfatning at en helhetlig tilnærming innen sikring av kritiske verdier, systemer, infrastrukturer og objekter, herunder skjermingsverdige verdier og objekter, er nødvendig for å unngå sub-optimalisering og unødig bruk av store ressurser.

Lov og forskrift peker flere steder på betydningen av at sektormyndigheter, forvaltere av kritiske verdier og eiere av kritiske systemer, infrastrukturer og objekter har adekvat trusselforståelse. Det er forsvarssektorens og justismyndighetenes ansvar å formidle trusselbildet – også gradert. Forskriftene bør etter FFIs syn i sterkere grad få fram krav til at trusselbildet og Forsvarets planlagte behov for støtte ved væpnet konflikt, formidles. Videre må mottakende myndigheter og eiere av kritiske verdier, systemer, infrastrukturer og objekter sette seg i stand til å motta slik informasjon.

Innspill og kommentarer til enkeltparagrafer i forslaget til de tre forskriftene

Til utkast til forskrift om myndighetens roller og ansvar for nasjonal sikkerhet (s.90 – 95)

§ 2 Bruk av adgangsklareringer
Kommentar: Til setningen «*Kan objektet eller infrastrukturen i stedet eller i tillegg være mål for spionasje eller sabotasje fra en annen stat, kan det fattes vedtak om utvidet adgangsklarering*.» FFI stiller spørsmål om dette kun skal gjelde dersom det er en annen stat som utgjør trussel om (spesifikt) sabotasje eller spionasje, eller også andre aktører. FFI oppfatter at myndighetenes rolle i stor grad vil være å vurdere konsekvenser av bortfall, altså skadepotensiale (ref. pkt 6.1.2 s. 32 i høringsnotatet). Det framstår som uklart hvorfor trussel i form av aktør og middel (stat, sabotasje og spionasje) her er spesifisert, da skadepotensialet ikke nødvendigvis er basert på dette.

FFI understreker også at terror, attentat, annen alvorlig kriminalitet, sabotasje og spionasje kan ha flere likhetstrekk. FFI mener at paragrafen bør unngå å bruke formuleringer og eksempler som faller utenfor virkeområdet til sikkerhetsloven, altså trusler som er på et nivå som ikke kan skade nasjonale sikkerhetsinteresser/GNF. Eksempelvis gjelder dette betegnelsen «annen alvorlig kriminalitet». FFI anbefaler derfor å vektlegge adgangskontroll for å unngå skade på GNF i paragrafen.

FFIs forslag til omformulering er gjort for enten å vektlegge at anslag fra en annen stat er hovedgrunnen til utvidet adgangskontroll, eller at spionasje og sabotasje er spesielt utpekt som trusler man bør ta hensyn til.

Forslag til formulering: «*Kan objektet eller infrastrukturen i stedet eller i tillegg være mål for tilsiktede anslag fra en annen stat, kan det fattes vedtak om utvidet adgangsklarering*.» ELLER «*Kan objektet eller infrastrukturen i stedet eller i tillegg være mål for spionasje eller sabotasje, kan/bør det fattes vedtak om utvidet adgangsklarering*.»

§ 3 Iverksettelse av inntrengningstesting, kommunikasjons- og innholdskontroll og testing av sikkerhetstiltak
I paragraf 3 henvises det ikke til sammenhengen mellom Nasjonal sikkerhetsmyndighet (NSM) sin rådgivende funksjon med tanke på bistand til gjennomføring av inntrengingstesting og testing «*Når virksomhetens leder ber om det*» og sikkhetsmyndigheten sin tilsynsrolle § 17. Noen av midlene nevnt i § 3 vil også være aktuelle for tilsyn, og det bør framgå klart når NSM (eller annen tilsynsmyndighet) har en tilsynsrolle, når de har en rådgivende rolle eller når det gjennomføres teknisk

sikkerhetsundersøkelse (TSU). Dette er for å unngå at § 3 kan være i motstrid til § 17 eller andre paragrafer.

§ 4 Iverksettelse av tekniske sikkerhetsundersøkelser
Det framstår som uklart om denne paragrafen gjelder kun enkeltrom som er sikret, eller også større områder og/eller infrastruktur. Dersom større områder også er inkludert her bør formuleringen «*rommet*» omskrives.

§ 8 Register over avgjørelser om personklarering
Det bør framgå av denne paragrafen hvor lenge «*informasjon om alle klareringsavgjørelser*» skal kunne være tilgjengelig. Dersom informasjonen skal være tilgjengelig for all framtid bør dette spesifiseres. (jf. § 69 i utkast til forskrift om virksomhetens arbeid med forebyggende sikkerhet: «*Dersom den autoriserte er klarert skal autorisasjonsopplysningene bevares i klareringens gyldighetstid*.» og «*Autorisasjonsansvarlig skal bevare taushetserklæring signert av den autoriserte og oversikter over personell som er eller har vært autorisert*, jf. § 63, *i 25 år*.»)

§ 9 Register over leverandørklareringer og sikkerhetsgraderte anskaffelser
Også i denne paragrafen (som over), bør det framgå hvor lenge «*register over alle leverandørklareringer*» skal kunne oppbevares.

Til utkast til forskrift om virksomhetens arbeid med forebyggende sikkerhet (s.96-112)

§ 5 Roller og ansvar i det forebyggende sikkerhetsansvaret
I paragrafens siste avsnitt står det: «*Kontroll av styringssystemer for sikkerhet skal om mulig utføres av andre enn de som har styrende eller utøvende oppgaver i det forebyggende sikkerhetsarbeidet*». I denne forbindelsen bør FDs trelinje forsvarsmodell danne utgangspunkt for kontrollfunksjonenes roller og samhandling innen virksomheter. Denne modellen bør være normgivende for innretningen av virksomhetenes sikkerhetsstyring. Virksomhetene bør etablere dedikerte 2.linjeressurser innen forebyggende sikkerhet, og disse må organiseres slik at det blir en klar rolleuavhengighet mellom 1.linjen (utøvelse), og 2.linjen (system-/kontrollansvar). En 2.linjeressurs innen forebyggende sikkerhet må ha virksomhetens leder eller dennes stedfortreder som foresatt.

§ 11 Plikt til å vurdere risiko
Denne paragrafen kan tolkes til å bety at det er virksomheten selv som kan velge hvilke trusler og risikoer de vil/skal vurdere. Her bør det også legges inn at virksomheten skal ta hensyn til nasjonale, regionale eller lokale risikoforhold, det være seg informasjon fra åpne eller graderte/delvis graderte kilder (PST, E-tjenesten eller NSMs risikovurderinger, DSBs krisescenarioer, Fylkes-ROS, kommunal ROS e.l.). Det bør henvises til andre paragrafer dersom dette kan oppklare pliktene til å vurdere ulike typer risiko, eller spesifiseres at virksomheten som minstemål skal inkludere spesifiserte risikoer eller trusler fra nasjonale eller overordnede myndigheter. For øvrig bemerkes det at det er svært positivt at det henvises til standardene ISO 31000, ISO/IEC 27001 og ISO/IEC 27005 i bakgrunnen for paragrafen.

§13 Grunnsikringstiltak, påbygningstiltak og tiltak for skadebegrensning og gjenopprettelse
Ett av grunnsikringstiltakene bør være at man har en handlingsplan av en viss kvalitet klar ved brudd på sikkerheten. Det står mye om påbyggingstiltak, planlegge skadebegrensningstiltak og plan for å gjenopprette et forsvarlig sikkerhetsnivå. Men en handlingsplan må dekke en analyse av mulige sikkerhetsbrudd og hvordan bedriften skal håndtere disse raskt og effektivt.

§14 Prinsipper ved valg og utforming av sikkerhetstiltak
Dersom et av sikkerhetstiltakene blir en handlingsplan (som nevnt over i §13) bør man her følge opp slik at denne handlingsplanen forstås i punktene.

I tillegg sier siste setning i paragrafen noe om "*inngripen i enkeltpersoners rettssikkerhet eller personvern*". Her (eller tidligere i forskriften) bør det komme fram at virksomheten må ha skriftlige rutiner/regler som følges ved utførelse av slik inngripen.

§ 17 Krav til sikkerhet i anskaffelser
Det anbefales å legge inn referanse til § 9 om leverandørklarering ifm. med krav til sikkerhet i anskaffelser.

§32 Forsvarlig sikkerhetsnivå for informasjon gradert KONFIDENSIELT eller høyere
I denne paragrafen fastslås det at uautoriserte personer ikke kan få tilgang til informasjon gradert STRENGT HEMMELIG. Selv om det ikke skal være mulig at uautoriserte personer får tilgang til slik informasjon, er det likevel nødvendig å ha en plan for å reversere skadene dersom STRENGT HEMMELIG informasjon kommer på avveie. Det er ikke tilstrekkelig å fastslå at dette ikke kan skje så lenge det er en mulighet for det. FFI anbefaler derfor at det bør stilles krav til virksomhetene at de har kriseplaner for å håndtere slike eventuelle situasjoner.

§44 Beskyttelse av rom og lokaler for tale gradert KONFIDENSIELT eller høyere
Begrep som protokoll vs. besøksoversikt bør harmoniseres. Det bør presiseres hva som er en tilstrekkelig besøksoversikt. Det kommer ikke klart fram om et besøk er noen som normalt ikke har tilgang til rommet, eller om det gjelder alle som er inne i rommet.

§45 Forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer
Kommentar: Denne paragrafen kan tolkes slik at det i hovedsak er dataene i informasjonssystemet som skal beskyttes. Dagens informasjonssystemer omfatter også systemer for adgangskontroll, alarm, overvåking, kontroll, styring, kommunikasjon osv. Alle disse kategoriene består av funksjonelt like komponenter, som fra et beskyttelsesperspektiv er likeverdige.

«*Informasjonssystemer*» er definert bredere i Stortingsproposisjonen, kap. 10.5.3.1 (s. 99), og i selve lovens Kap. 6 § 6-1: «*Et informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner*.»

Hvilke trusler informasjonssystemene skal beskyttes mot, diskuteres i kommentarene til forskriften (for eksempel s.61 osv.). Det framgår der at det er dataenes integritet og tilgjengelighet, så vel som tjenester, som skal opprettholdes. Isolert sett, uten støtte fra kommentarer og forarbeider, kan forslaget til forskrift gi for snevre assosiasjoner.

Forslag til omformulering: (siste avsnitt etter pkt. g) Alle endringer er markert i kursiv.
Når virksomheten vurderer hvordan risikoen skal håndteres, skal den ta utgangspunkt i hvilken betydning informasjonssystemet har for grunnleggende nasjonale funksjoner. «*Betydningen kan være direkte når informasjonssystemet selv håndterer skjermingsverdige data eller utfører tjenester. Tilsvarende kan betydningen være indirekte i tilfeller hvor informasjonssystemet understøtter skjermingsverdige data eller tjenesters integritet ved påvirkning av randbetingelser eller miljø».*

Sikkerhetstiltakene skal være tilpasset systemets totale omfang og kompleksitet gjennom hele systemets levetid, «*og dekke det relevante spekteret av fysiske, elektromagnetiske og nettbaserte trusler».*

Sikkerhetstiltak som skal virke hurtig, eller som lett kan utløse feil når de utføres manuelt, skal automatiseres.

§ 48 Godkjenningen
Kommentar: Paragrafen starter med følgende setning «*Godkjenningen er en planlagt og systematisk gjennomgang av at virksomheten, for å oppnå et forsvarlig sikkerhetsnivå for informasjonssystemet, på en tilfredsstillende måte har vurdert og håndtert risiko ved å ha…*». For å klargjøre budskapet i denne paragrafen ytterligere forslår FFI en omformulering.

Forslag til formulering: «*Godkjenningen er en planlagt og systematisk gjennomgang av at virksomheten på en tilfredsstillende måte har vurdert og håndtert risiko for å oppnå et forsvarlig sikkerhetsnivå for informasjonssystemet, ved å ha…*».

Overskrift: Kapittel 7. Beskyttelse av skjermingsverdig objekter og infrastruktur
FFI foreslår å endre kapittel 7 overskriften fra: «*Beskyttelse av skjermingsverdig objekter og infrastruktur*» til «*Beskyttelse av skjermingsverdige objekter og infrastrukturer*». Både objekter og infrastruktur er flertallsord i denne sammenhengen.

§ 52 Skadevurdering i forbindelse med klassifisering av skjermingsverdig objekter eller infrastruktur
I § 52 er det et avvik mellom kommentarene til paragrafene (s.66-67) og selve paragrafen. I følge kommentarene skal paragrafen inneholde ledd a-e, men i selve paragrafen mangler det som refereres til som «ledd d» om avhengigheter. Bokstav d avviker for øvrig fra resten av vurderingene som skal gjøres, «*hvilken grad rettstridig overtakelse av objektet- eller infrastrukturen kan påvirke befolkningens grunnleggende sikkerhet*.» Bokstav a-c henges opp i GNF, og FFI mener at dette også bør gjelde bokstav d. Befolkningens grunnleggende sikkerhet skal være en del av vurderingen for utpeking av GNF, og dermed hører vurderingen hjemme i utpekingen av GNF, ikke nødvendigvis i vurderingen av objekter eller infrastrukturer direkte. Dersom dette skal være et eksplisitt utpekt vurderingskriterium innen skadevurdering, må dette begrunnes bedre. Alternativt kan man legge inn en forventning om vurdering av alle kategoriene i nasjonale sikkerhetsinteresser bokstav a-e (Prop. 153 L s.34) i en skadevurdering.

§57 Virksomheters rett til innsyn
Retten til innsyn kommer klart fram i denne paragrafen, men det kommer ikke klart fram hvordan varslingssystemet for digital infrastruktur (VDI) kan benyttes og eventuelt videreformidle data senere. Dette bør komme klart fram av forskriften, eller så bør det uttrykkelig skrives at dette reguleres av avtalen mellom VDI og virksomheten.

Prinsippet om minimum eksponering av skjermingsverdig informasjon bør følges. Omfang og lagring av informasjon skal minimeres. Dette kan forklares med lavere risiko for informasjon på avveie, og lavere krav til lagring og viderebehandling av data under punkt 7.9.2 (s.70) i kommentarene til forskriften.

Til utkast til forskrift om klarering av leverandører og personell (s. 113-121)

Overordnet til forskriften
Forskriftene om klarering av personell tar i liten grad inn over seg konsekvensene for personer som ikke blir klarert eller reklarert. Manglende reklarering kan føre til at ansatte mister jobben. Forskriftene bør si noe om hva som skjer når man ikke får klarering, hvilke rettigheter har den ansatte, klagemuligheter etc.

§ 1: Misvisende bruk av «sivil sektor».
Til setningen «*Forsvaret klarerer personell i forsvarssektoren. Sivil klareringsmyndighet klarerer personell i sivil sektor.*» FFI anbefaler å unngå bruken av begrepet «sivil sektor».

Forsvarsdepartementet, som eksempel, er en del av forsvarssektoren, men det er også et sivilt departement. «Sivil sektor» kan som sådan omfatte de andre departementene og underlagte etater, eller også inkludere FD dersom «sivil sektor» refererer til alt som ikke er militær organisasjon. Det anbefales heller å bruke begreper som «andre sektorer», «sivile sektorer» eller «personell utenfor forsvarssektoren».

§ 7: Krav til egenopplysninger
I forskriftsteksten stilles det krav til hvilke opplysninger som skal gis av den som skal sikkerhetsklareres, mens det i kommentarene diskuteres mulighet for automatisk innhenting av mange av disse opplysningene. Automatisering og effektivisering hos klareringsmyndigheten kan her komme i konflikt med de oppgavene som skal utføre lokalt i virksomheten innen den daglige sikkerhetsmessige ledelse. Vi anser det som viktig med et så godt grunnlag som mulig, med førstehåndsinformasjon fra hovedpersonen selv, for å kunne gjennomføre de oppgavene som tilligger autorisasjonsansvarlig og virksomhetens ledere.

Med hilsen

Jan Erik Torp
Stabssjef

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Vedlegg til Høring - Forskrifter til ny sikkerhetslov
Svar på spørsmål i høringsnotat «Forslag til forskrifter til ny sikkerhetslov» fra FFI

I høringsnotatet stilles det en del eksplisitte spørsmål som Forsvarsdepartementet ønsker svar på. Disse besvares under:

1. Side 11: Inndeling i forskrifter. Spørsmål om inndelingen i forskrifter er hensiktsmessig.
    a. Inndelingen i tre forskrifter virker hensiktsmessig og oversiktlig.
2. Side 11: Innspill til korttitler. Innspill til offisielle korttitler for å sikre at disse er tilstrekkelig entydige.
    a. Korttitlene som de står nå gir mening.
3. Side 13: Objekt- og infrastruktursikkerhet. Dept. ber høringsinstansenes syn på om det bør gis mer detaljerte krav til sikring av infrastruktur, og i så fall hvilke krav bør stilles.
    a. Se FFIs høringssvar.
4. Side 20: § 8-7. Dept. ber imidlertid om høringsinstansenes innspill på om det er behov for en bestemmelse som konkretiserer vurderingstemaene ytterligere, og vil vurdere en slik bestemmelse i lys av høringsinnspillene.
    a. FFI støtter FDs og NSMs syn på at det bare unntaksvis skal tillates klarering av utenlandske statsborgere uten tilknytning til Norge. Det som er viktig er at prosessen fram til klarering foreligger er godt dokumentert og risikovurdert hos virksomhetene.
    b. Tilgang til NSMs landvurderinger vil måtte være en del av verktøyet her.
5. Side 22: § 11. Dept. ber derfor om høringsinstansenes syn på behovet for og hensiktsmessigheten av den unntaksbestemmelsen som er foreslått i myndighetsforskriften § 11, og vil vurdere bestemmelsen i lys av høringsinnspillene.
    a. Vi vurderer § 11 som en klargjøring av de andre relevante §§. Denne mener vi det kan være et behov for, og at hensikten må være å klargjøre myndighetsansvaret og muligheten for å kunne gjøre unntak fra klareringsbestemmelsene.
6. Side 24: § 9-4. Dept. ber om høringsinstansenes innspill på om det er nødvendig med ytterligere forskriftsbestemmelser knyttet til denne bestemmelsen.
    a. Vi ser ikke at det er nødvendig med ytterligere forskriftsbestemmelser.
7. Side 25: § 9-3. Dept. ber om høringsinstansenes syn på hvem som bør være klareringsmyndighet for leverandørklarering.
    a. Forslaget om bruk av sivil klareringsmyndighet for leverandørklareringer synes riktig i og med at NSM vil være tilsynsmyndighet for både leverandørene og oppdragsgiverne ved sikkerhetsgraderte anskaffelser. Vi tilslutter oss forslaget om endring her.
    b. Sikkerhetsansvarlig for anskaffelsen videre i prosessen vil være den som NSM utnevner.
8. Side 26: Ikrafttredelse. Dept. ber om høringsinstansenes innspill, og vil vurdere en slik bestemmelse i lys av høringsrunden.
    a. Vi vurderer det som hensiktsmessig at virksomhetene får konkrete momenter å forholde seg til når det settes en frist for å oppnå målet om forsvarlig sikringsnivå.
9. Side 32: § 52. Dept. ber om høringsinstansenes syn på om ovennevnte kriterier er tilstrekkelige for at dept skal kunne beslutte et klassifiseringsnivå etter sikkerhetsloven § 7-1.
    a. Se FFIs høringssvar.
10. Side 33: § 6. Dept. ber høringsinstansenes syn på om bestemmelsen gir tilstrekkelige føringer for å benytte tredjepart til disse oppgavene, og ønsker særlig tilbakemelding på om det bør fremgå ytterligere kriterier, og i så fall hvilke, som bør fremgå av forskrift for bruk av tredjeparter i disse tilfellene.

a. Et kriterie kan være at virksomheten må være norsk eid og være plassert i Norge, hvis dette ikke kommer i konflikt med andre regelverk.
b. I tillegg kunne det stå spesifikt at personell som skal utføre oppgaver for tredjepart må kunne klareres og autoriseres for STRENGT HEMMELIG, hvis dette da ikke skal vurderes når oppdragets art og innhold er klarlagt. Det kommer ikke fram i forskriften om dette er noe som skal vurderes for det enkelte oppdrag eller når tredjepart blir utnevnt.
c. Vi er i utgangspunktet skeptisk til å la tredjepart utføre tekniske sikkerhetsundersøkelser fordi den kompetansen og den kunnskapen som tredjepart tilegner seg, er kritisk i forhold til deling av kunnskap om etterretningsmetoder og avlytting.
d. En annen risiko er at virksomhetens (tredjeparts) økonomi kan bli styrende for kvaliteten på undersøkelsene.
e. Hvor lenge skal en slik avtale gjelde? Krav til utlysning, anbud etc?

11. Side 36: Kapittel 4 Tilsyn. Dept. ber høringsinstansene om deres synspunkter på innholdet i bestemmelsene og ønsker også synspunkter på om det er noe av dette som bør stå i forskrift av hensyn til forutberegnelighet for de som blir gjenstand for tilsyn.
    a. Vi anser det som hensiktsmessig at kapittel 4 om tilsyn blir stående i forskriftsform som i forslaget.
12. Side 40: § 20. Dept. ber om høringsinstansenes innspill til bestemmelsen, og vil vurdere behovet for ytterligere bestemmelser om eierskapskontroll i lys av høringsinstansenes innspill. Dept. vil også vurdere om det er mer hensiktsmessig at bestemmelsen fremgår av virksomhetsforskriften.
    a. Ingen innspill til innhold.
    b. Bestemmelsen vurderes fra oss til mer naturlig å høre inn under virksomhetsforskriften.
13. Side 42: Forsvarlig sikkerhetsnivå. Dept. ber særlig om høringsinstansenes innspill på denne innretningen for hvordan en virksomhet kan beskytte sine skjermingsverdige verdier på en slik måte at kravet til forsvarlig sikkerhetsnivå oppnås.
    a. Forsvarlig sikkerhetsnivå skal i framtiden vurderes av hver virksomhet opp mot fysisk, elektronisk, menneskelig eller organisatorisk sikringstiltak. FFI mener dette blir en utfordring fordi det i mangel av konkrete forslag til sikring slik dagens forskrift legger opp til, blir hver enkelt virksomhets leder som beslutter sin virksomhets nivå basert på egen risikoerkjennelse og situasjonsforståelse. Gjørv-kommisjonen påpekte i sin rapport at nettopp erkjennelse av risiko er og blir en utforing siden dette er subjektivt. Det som blir utfordringen da er at samme objekt vil kunne ende opp med ulike nivåer av sikringstiltak. FFI anbefaler at forskriftene gjøres mer spesifikke i forhold til hva som forventes slik at store variasjoner i sikringsnivå unngås.
14. Side 42: § 1 Definisjoner. Dept. ber om høringsinstansenes syn på om definisjonene i bestemmelsen er nødvendig, og på om det er andre begreper som bør defineres.
    a. Det er hensiktsmessig at definisjonene beskrives som vist i forslaget.
    b. Med referanse til neste punkt så kan det også være hensiktsmessig å ha med definisjonen for sikkerhetstruende virksomhet under § 1.
15. Side 46: § 7. Dept. ber høringsinstansenes syn på bruken av begrepet «sikkerhetstruende virksomhet».
    a. Det er etter vår mening et innarbeidet begrep som kan videreføres. Viktig med definisjon som nevnt i punktet over under § 1.
16. Side 47: § 12. Dept. ber særlig om høringsinstansenes syn på denne innretningen.
    a. Som beskrevet i høringsnotatet kan setningen nedenfor legges til i § 12 slik at informasjonen med en gang er tilgjengelig for leseren, før leseren benytter de tilhørende §§ for å håndtere de

nødvendige risikoene: «Håndteringen av risiko avhenger av den skjermingsverdige verdiens betydning for grunnleggende nasjonale funksjoner (klassifiserings- og graderingsnivå).»

17. Side 59: § 38. Dept. ber om høringsinstansenes innspill på om dette er en hensiktsmessig innretning, og hvorvidt det finnes anerkjente standarder eller metoder som bør ligge til grunn for godkjenning av oppbevaringsenheter.
    a. Vi mener at dagens ordning bør videreføres.
18. Side 64: § 48. Dept. ber om innspill på om godkjenningsbestemmelsen er hensiktsmessig utformet.
    a. Se FFIs høringssvar.
19. Side 69: § 56. Dept. ber om høringsinstansenes syn på en slik påleggskompetanse, og eventuelt hvilke rammer en slik påleggskompetanse bør ha.
    a. Det kan være at man per nå ikke har fullstendig oversikt over hvilke konsekvenser ressursmessig og i praksis et slikt pålegg vil ha. Vi kjenner ikke til hva som eventuelt er kartlagt i forhold til omfang eller ressurser etc. Det kan være at NSM skal kunne ha mulighet til å pålegge en slik tilknytning i tilfeller der myndighetene ser at dette er ønskelig og hensiktsmessig, men at det ikke er pålegg om dette for alle.
20. Side 76: §1 Klareringsmyndighet. Dept. ber om høringsinstansenes syn på femte ledd.
    a. Se FFIs høringssvar.
    b. Vi er enige med dept. i at personer som skal klarere andre bør ha minimum samme klareringsnivå som de personene de skal fatte klareringsvedtak om. Dette bør stå i forskriften for lik praksis.
21. Side 81: § 16 Vurderingsgrunnlag. Dept. ber om høringsinstansenes innspill til bestemmelsen, herunder om momentene i tilknytningsvurderingen bør fremgå tydeligere av forskriftene.
    a. Her kunne man i tillegg henvise til at klareringsmyndighetene skal legge NSMs personellsikkerhetsmessige vurderinger av andre stater til grunn, slik at dette står i forskriften og sikrer likebehandling.
    b. Angående landvurderinger: For virksomheter som driver utstrakt proaktiv sikkerhetstjeneste som ledd i å sikre kritiske nasjonale verdier, bør det åpnes for at NSM deler landvurderingene med disse virksomhetene. Det er viktig at virksomhetene kan benytte landvurderingene i forbindelse med reisesamtaler, vurdering av autorisasjon og annen forebyggende sikkerhetstjeneste.
22. Side 84: § 26 Samtykke. Dept. ber derfor om høringsinstansenes innspill, og vil vurdere etter høringsrunden hvorvidt det er hensiktsmessig å videreføre bestemmelsene i kapittel 4. Et alternativ er at virksomhetene blir gjort kjent med NSMs vurdering av andre stater, jf. § 16.
    a. Forespørselen bør gå via personellsikkerhetsansvarlig i virksomheten. (Det vi i dag kaller anmodende myndighet).
    b. Personellsikkerhetsansvarlig bør få tilgang til NSMs landvurderinger for å kunne vurdere en slik anmodning til klareringsmyndigheten i forkant. En mulighet for å kunne gjøre en slik vurdering vil gjøre at man unngår å sende inn anmodninger som det av sikkerhetsmessige grunner ikke er ønskelig å gjøre fra anmodende myndighets vurdering.