Remissvar: MSB konsekvensutredning avseende föreskrifter om säkerhetsåtgärder (MSB 2025-13269)

1. Sammanfattning

Bedömningen är att utredningen lider av så pass allvarliga brister i kostnadsanalys och metodik att den inte kan ligga till grund för beslut. Kritiken sammanfattas i fyra huvudpunkter:

1. **Utgångspunkt i informationssäkerhet i stället för CSL krav på cybersäkerhet.:** CSL syfte är en hög nivå av cybersäkerhet i samhället (CSL 1 kap 1 §), Cybersäkerhet definieras som skyddet av nätverks- och informationssystem, användarna av dessa system och andra personer mot cyberhot. Skydd av samhällsviktiga funktioner. MSB fokuserar helt på informationssäkerhet, skydd av information. Detta felgrepp gör att EU intentioner och EU-rätten runt cybersäkerhet helt frångår. Informationssäkerhetsåtgärder kan motverka cybersäkerheten.
2. **Oredovisade miljardkostnader:** Utredningen missar helt de massiva kostnader som kravet i utredningen medför. Det är allt från kostnader för spårbarhet och informationsklassning till kostnader för fysiskt åtskilda sektioner och kostnader för tidhållning.
3. **Tekniska särkrav och Inlåsning:** Kravet på nationell tidssynkronisering (UTC SP) och implicita krav på ISO 27001-certifiering skapar unika svenska handelshinder. Detta omöjliggör användning av standardiserade molntjänster och global hårdvara,.
4. **Bristande utredning av alternativ:** MSB har underlåtit att utreda det mest kostnadseffektiva alternativet: att direkt tillämpa EU:s genomförandeförordning och använda ENISA:s tekniska vägledning. Detta vägval skulle eliminera behovet av dyra nationella särlösningar och harmonisera svenska krav med övriga Europa.

Sammanfattningsvis riskerar MSB:s förslag att skapa en tung administration som tar bort fokus från det faktiska säkerhetsarbetet, vilket i förlängningen försvagar snarare än stärker

För att säkerställa att CSL implementeras effektivt och utan att skada svensk konkurrenskraft, rekmmenderas följande:

1. **Använd genomförandeförordningen:** Uppdatera genomförandeförordningen med CSL-terminologi och låt denna utgöra grunden för föreskrifterna. Detta eliminerar behovet av kostnadsdrivande särkrav.
2. **Använd ENISA:s Tekniska Implementationsguide:** Översätt ENISA:s tekniska guide till svenska och för in CSL-terminologi. Detta ger svenska företag omedelbar tillgång till högkvalitativt metodstöd till en bråkdel av kostnaden för egenutveckling.

2. MSBs missförstånd att Cybersäkerhet och Informationssäkerhet är samma sak

Kärnan i bristerna ligger i en begreppsförvirring. MSB likställer i konsekvensutredningen sid 4 cybersäkerhet med informationssäkerhet. Det är fel. Två ord, "av" samt "och" finns i båda definitionerna. Syftet är olika, att MSB saknar förståelse för skillnaden är ett stort problem.

- NIS2/CSL: Syftar till att skydda nätverks- och informationssystemens förmåga att upprätthålla samhällsviktiga tjänsters funktion.
- MSB:s Föreskrift: Fokuserar på klassificering och skydd av informationstillgångar.

Denna begreppsförvirring leder till felaktiga prioriteringar i kravställningen. Om en åtgärd för att skydda informationens konfidentialitet (t.ex. kryptering eller komplex inloggning) hotar systemets tillgänglighet, så motverkar åtgärden NIS2-direktivets primära syfte. MSBs begreppsförvirring leder till att föreskrifterna bryter mot lagens intention.

3. Systematiskt och riskbaserat arbete

Sid 5 i konsekvensutredningen rör "systematiskt och riskbaserat arbete". Återinförandet av kravet på "systematiskt och riskbaserat arbete" med hänvisning till ISO 27000 utgör en implicit tvingande certifiering.

1. Dubbelreglering: I propositionen till CSL bedömdes detta krav vara överflödigt då det redan följer av lagens allmänna säkerhetskrav. Att MSB återinför det i föreskrift skapar osäkerhet och dubbla revisionskrav.
2. Kostnad: Full implementering och certifiering mot ISO 27001 kostar för ett medelstort företag ofta mellan 1–5 miljoner kronor. Detta är en kostnad som MSB i sin utredning betraktar som "försumbar" eller redan tagen, vilket inte stämmer.

4. Analys av Alternativa Lösningar

Enligt 6 § förordningen om konsekvensutredningar ska myndigheten redovisa vilka alternativa lösningar som övervägts. MSB avfärdar alternativet "Inga föreskrifter" (sidan 6-8) men underlåter att utreda att direkt tillämpa EU:s genomförandeförordning med CSL-terminologi.

Om MSB hade valt detta spår hade följande kostnader eliminerats:

- Inga särkrav: Kostnader för UTC (SP), fysisk separation och specifika roller försvinner.
- Gratis metodstöd: Svenska företag hade direkt kunnat nyttja ENISA:s "Technical Implementation Guidance" och dess mappningstabeller mot ISO 27001, vilket hade sparat stora belopp i konsultkostnader för tolkning av unika svenska regler.

Att inte kvantifierar besparingen med detta alternativ utgör en stor brist i beslutsunderlaget.

4. Avsaknad av spårbarhet mot CSL

Egen terminologi och struktur gör att genomförandeförordningens mappning mot NIS2 / CSL inte kan användas. På sid 9-10 ges en övergripande redovisning av hur lagkraven förtydligats och konkretiserats. Detta sätt att beskriva spårbarhet saknar legalt värde.

Verksamhetsutövarna måste själva skapa spårbarhet.. Kostnaderna för detta är höga men svåröverskådliga. MSB saknar kostnadskalkyl.EU:s cybersäkerhetsbyrå ENISA har publicerat *"Technical Implementation Guidance on Cybersecurity Risk Management Measures"*. Detta dokument på 170+ sidor innehåller detaljerade mappningstabeller mot ISO 27001, konkreta exempel på bevisbörda och tekniska specifikationer.

5. Organisatoriska kostnadsbedömningar

5.1. Informationsklassning

Kravet att klassificera information före riskanalys pekas ut som det enskilt mest kostnadsdrivande administrativa momentet.

- Arbetsinsats: För en medelstor kommun eller region med miljontals dokument och datapunkter innebär detta tiotusentals arbetstimmar.
- Relevans: Uppskattningsvis 90–95 % av denna information saknar relevans för *kontinuiteten* i de samhällsviktiga tjänsterna (t.ex. vattenförsörjning eller elnät).

För en verksamhet med 20 års datahistorik är det inte bara dyrt, det är *omöjligt* att klassa allt retroaktivt utan att lamslå verksamheten. Detta är ett oproportionerligt krav.

5.2 Kostnaden för staten: Egenutveckling vs. Översättning

Konsekvensutredningen redovisar inte kostnaden för MSB att ta fram det stödmaterial som krävs för att göra de unika svenska föreskrifterna begripliga och tillämpbara.

- Alternativ 1 (MSB:s väg): Att ta fram och förvalta en svensk teknisk handbok som håller samma kvalitet som ENISA:s (170 sidor expertmaterial) är ett omfattande arbete. MSB nuvarande stöd för informationssäkerhet stödjer inte cybersäkerhet enligt CSL och ligger mycket långt från det stöd och den spårbarhet som ENISA ger.
- Alternativ 2 (Harmonisering): Att istället översätta och anpassa ENISA:s befintliga guide till svenska skulle kosta en bråkdel. En professionell facköversättning och granskning estimeras till < 0,5 miljoner kronor.

Slutsats: Genom att inte välja "översättningsspåret" påför MSB staten en onödig utvecklingskostnad på tiotals miljoner och näringslivet en kostnad i form av sämre och senare vägledning. Denna samhällsekonomiska förlust borde ha belysts i konsekvensutredningen.

6. Tekniska kostnadsbedömningar

6.1 Underskattning av Infrastrukturkostnader (Fysisk Separation)

På sid 13 i konsekvensutredningen,"Fysiska säkerhetsåtgärder", anges att kostnaden för att inrätta *"fysiskt åtskilda sektioner"* uppskattas till 50 000 – 150 000 kr per sektion.

Denna kalkyl är en grov underskattning för verksamheter med kritisk infrastruktur (t.ex. elnät, vattenverk). Kravet i föreskriftens 12 kap. 19 § om att placera redundanta system i fysiskt åtskilda sektioner innebär i praktiken ofta nybyggnation av teknikhus eller omfattande ombyggnation av ställverk för att uppnå separata brandceller och fysiskt skydd.

- Verklig kostnad: En realistisk kostnad för ett nytt, fysiskt separerat teknikhus med kyla, kraft och skalskydd är 1 – 3 miljoner kronor per enhet.
- Konsekvens: För en nätägare med 100 anläggningar innebär MSB:s kalkyl en kostnad på ca 10 MSEK, medan den verkliga kostnaden kan uppgå till 200–300 MSEK. Denna diskrepans ogiltigförklarar utredningens slutsats om proportionalitet.

6.2 Felkalkylering av Tidshållning (UTC SP)

På sid 16 bedöms investeringen för *"robust och spårbar tid"* (kravet på UTC SP) till 30 000 – 200 000 kr. MSB bortser från komplexiteten i moderna hybridmiljöer:

- Teknisk inlåsning: Globala molntjänster och standardiserad nätverksutrustning använder globala källor (GPS/USNO). Spårbarhet mot UTC SP saknas. MSB:s krav gör det olagligt för svenska berörda aktörer att använda standardiserade molntjänster.
- Integrationskostnad: Kostnaden ligger inte i hårdvaran, utan i att bygga och förvalta speciallösningar för att tvinga in svensk tid i globala system. Driftskostnaden och risken för tekniska problem vid uppdateringar har helt utelämnats i kalkylen.

7. Analys av andra EU-länder

För att bedöma rimligheten i MSB:s förslag är det nödvändigt att jämföra med hur andra medlemsstater implementerar NIS2. Analysen visar att Sverige väljer en väg av detaljreglering som avviker från den europeiska normen av ramverksstyrning.

7.1 Belgien: Cyberfundamentals (CyFun)

Belgien har valt en pragmatisk modell genom ramverket Cyberfundamentals (CyFun).

- CyFun mappar direkt mot NIS2, ISO 27001, NIST CSF och IEC 62443.
- Det finns inga krav på unika nationella roller eller tidsstandarder.
- Genomförandeförordningen för digitala leverantörer tillämpas direkt utan nationella tillägg, vilket garanterar en "level playing field".[6]

7.2 Irland: NCSC RMM

Irland, som är navet för många digitala tjänster i EU, har publicerat "Risk Management Measures" (RMM).

- Viktigt är att irländska NCSC explicit anger att entiteter som omfattas av EU:s genomförandeförordning ska följa denna *istället* för de nationella RMM 003–014. Detta eliminerar risken för motstridiga krav.
- Sveriges förslag saknar en sådan tydlig "carve-out", vilket riskerar att placera svenska moln- och datahallleverantörer i en omöjlig sits där de måste följa både EU:s förordning (för sina europeiska kunder) och MSB:s särkrav (för sina svenska kunder).

7.3 Tyskland: Differentiering för KRITIS

Tyskland ställer mycket höga krav, men gör det genom en tydlig differentiering.

- De strängaste kraven (t.ex. system för angreppsdetektering, SzA) gäller enbart för "Kritische Anlagen" (KRITIS), en delmängd av väsentliga entiteter.
- MSB:s förslag tenderar att applicera höga krav (som informationsklassning och fysisk separation) brett över alla väsentliga och viktiga entiteter, snarare än att rikta dem mot de mest kritiska anläggningarna