

SME-D

Justitiedepartementet
103 33 Stockholm

Yttrande över betänkandet En ny Säkerhetsskyddslag (SOU 2015:25)

Justitiedepartementet har genom remiss bjudit in SME-D att lämna synpunkter på betänkandet SOU 2015:25 En ny Säkerhetsskyddslag.

SME-D ställer sig positiv till en moderniserad Säkerhetsskyddslag.

SME-D vill ur förslaget lyfta fram den internationella anpassningen samt ett ökat informationssäkerhetsfokus som de mest angelägna förändringarna av nuvarande lagstiftning.

SME-D redovisar nedan synpunkter – framförallt ur ett SME-perspektiv – på föreliggande betänkande.

1.12 Förslag till säkerhetsskyddsförordning

I författningsförslagets 4 kap. 3§ föreslås att IT-system som av flera personer ska användas för bearbetning av säkerhetsskyddsklassificerade uppgifter ska vara försett med funktioner för skydd av bland annat röjande signaler.

SME-D anser att förslaget kring röjande signaler bör förtydligas och att kravet endast tillämpas på IT-system som hanterar högre informationssäkerhetsklasser.

SME-D anser vidare att internationella principer (Tempest) bör gälla framför svenska särlösningar (röjande signaler, RÖS) och att ett förtydligande görs för att inte exkludera Tempest-lösningar.

Det skulle vara mycket kostnadsdrivande för myndigheter och företag att införskaffa RÖS-godkänd datorhårdvara för att bearbeta säkerhetsskyddsklassificerade uppgifter i de lägre informationssäkerhetsklasserna. Enligt SME-D skulle kostnaden för att införa kravet vida överstiga nyttan.

Standardiserade och allmänt vedertagna metoder och teknologier för säkerhetsskydd håller nere kostnaderna för skyddsåtgärder. I fallet med röjande signaler bör således internationella principer (Tempest) gälla för att inte svenska särlösningar ska bli kraftigt kostnadsdrivande.

15.3 Informationssäkerhetsklasser – grunden för skydd av säkerhetsskyddsklassificerade uppgifter

SME-D välkomnar förslaget att använda fyra informationssäkerhetsklasser.

SME-D anser dock att Försvarsmaktens nuvarande system för informationsklassificering ska tjäna som modell för samtliga myndigheter.

SME-D anser vidare att en harmonisering mellan Sveriges och övriga EU-länders syn på informationssäkerhetsklassificering är nödvändig.

Det finns tydliga fördelar med att ha en myndighetsgemensam informationsklassificering och att inte Försvarmakten (som är den myndighet som hanterar flest informationsklassificerade uppgifter) har en egen.

Att använda de svenska benämningar Konfidentiell istället för HEMLIG/CONFIDENTIAL skulle öka osäkerheten och risken för att klassificerad information hanteras på ett felaktigt sätt. Inom privata företag är det vanligt att klassa dokument som *konfidentiell* utan att det avser försvarssekretess. Samma risk finns med att använda *begränsad* istället för HEMLIG/RESTRICTED.

Det är mycket angeläget att ett liknande synsätt på de olika informations-säkerhetsklasserna finns inom EU. Idag upplever SME-D att kravställning för skydd av framförallt HEMLIG/RESTRICTED kraftigt överstiger de flesta – möjligen alla – andra EU-ländernas krav. Detta innebär komplexa och kostnadsdrivande lösningar i Sverige som dessutom inte är konkurrenskraftiga för svensk industri inom resten av EU.

19.2 Säkerhetsskyddsavtal

SME-D förordar att enskilda tillåts använda säkerhetsskyddad upphandling för säkerhetskänslig verksamhet och att enskilda kan ingå säkerhetsskyddsavtal direkt med leverantör utan att avtalet ingås av staten, företrätt av en myndighet.

SME-Ds bedömning är att en trepartskonstruktion medför en ökad komplexitet och med ökad risk att de tre parterna blir oense avseende kravuppfyllnad.

20 Internationell samverkan

SME-D ställer sig tveksamt till att Försvarmakten ska få ett utökat ansvar för internationell samverkan inom säkerhetsskydd. Regeringen bör ytterligare utvärdera resultaten av dagens ordning innan Försvarmakten förordnas som nationell säkerhetsmyndighet.

SME-D anser att rekommendationer i utredningen NISU 2014 i tillämpliga delar bör lyftas in i den nya säkerhetsskyddslagstiftningen.

SME-D ställer sig positiv till att lagstiftningen tydligt pekar ut Försvarets materielverk som industrisäkerhetsmyndighet.

SME-D delar inte utredningens beskrivning av att Sveriges internationella samarbete på området för säkerhetsskydd i allt väsentligt fungerar väl. I avsnitt 20.2 beskriver utredningen kort funktioner för informationssäkring, kryptografisk säkerhet och industrisäkerhet enligt dagens ordning där Försvarmakten har särskilda uppdrag inom bland annat godkännande och distribution av kryptografisk material.

SME-D upplever inte att Försvarmakten ser som sin kärnverksamhet att driva internationell samverkan inom säkerhetsskyddsområdet och är därför tveksamt

till att myndigheten ska få utökade uppgifter innan effekterna av dagens ansvar utretts mer grundligt.

Utredningen NISU 2014 är en ambitiös ansats för att förbättra den rådande situationen med allvarliga brister inom informationssäkerhetsområdet. Det är därför naturligt att den nya säkerhetsskyddslagen (med ett uttalat fokus på bland annat informationssäkerhet) tar till vara på NISU-utredningens rekommendationer som i stor utsträckning även är relevant för det mest skyddsvärda i Sverige. Reglering i lag skulle sannolikt minska de allvarliga bristerna inom informationssäkerhetsområdet som i olika utredningar konstaterats under många år.

Ett tydliggörande att Försvarets materielverk fullt ut ska ansvara för industrisäkerhetsfrågor är välkommet. Enligt SME-D bör det dock tydliggöras – i lag eller regleringsbrev – att dels en harmonisering med övriga europeiska industrisäkerhetsmyndigheter är nödvändig, dels att Industrisäkerhetsmyndigheten även bör vara behjälplig med internationella säkerhetsskyddsfrågor vid svensk export. Detta skulle då utgöra en del i en exportfrämjande verksamhet till nytta för svenskt försvar och säkerhet, även om det inte direkt berör bilaterala projektöverenskommelser.

21.1 Tillsynens inriktning och genomförande – bör sanktioner införas?

SME-D anser att tillsynsmyndigheter ska få mandat att utfärda sanktioner vid konstaterade allvarliga brister i säkerhetsskyddet.

Riksrevisionen har i sin granskningsrapport angående Informationssäkerheten i den civila statsförvaltningen (RIR 2014:23) gett uttryck för att allvarliga brister i bland annat tillsyn och uppföljning inte föranlett förbättringar under de sju år som passerat sedan föregående granskning. Detta visar tydligt på behovet av kraftfulla åtgärder för att säkerställa säkerhetsskyddet – åtminstone avseende informationssäkerheten.

Riksrevisionen rekommenderar regeringen att överväga att låta tillsynsmyndigheter få mandat att utfärda sanktioner mot myndigheter som inte vidtar åtgärder efter konstaterade brister. SME-D förespråkar att en sådan sanktionsrätt omhändertas i den nya Säkerhetsskyddslagstiftningen för att slutligen komma till rätta med dagens allvarliga brister inom delar av säkerhetsskyddet.

Vänliga hälsningar



Magnus Sjöland
Ordförande

The Swedish Association of Small and Medium Size Enterprises
in Defense and Security