

		1 (2)
	Datum	
	Datum	Er referens/diarienummer
	2021-01-25	Fö2020/00954
Avsändare		Mottagare
Anders Lindberg, 08-555 520 84, anders.lindberg@sis.se		Försvarsdepartementet

Svar på remiss: EU:s cybersäkerhetsakt - kompletterande nationella bestämmelser om cybersäkerhetscertifiering – SOU 2020:58

Synpunkter på utredningen

Svenska institutet för standarder, SIS, har via Sveriges Standardiseringsförbund getts möjlighet att svara på remissen, och önskar lämna ett yttrande. SIS yttrar sig i frågor som rör standardisering som process samt hänvisning till standarder och tekniska specifikationer, genom SIS roll som nationellt standardiseringsorgan. I vår bedömning av remissen har vi ett standardiseringsperspektiv med fokus på informationssäkerhet.

I utredningen beskrivs standarder som ”frivilliga verktyg som ger hjälp att följa lagstiftningen” (s 79, fotnot nr. 60). SIS önskar fylla ut och nyansera beskrivningen. Standarder kan beskrivas som frivilligt och i samförstånd framtagna gemensamma lösningar på ofta återkommande problem. Standarder ska inte vara i konflikt med lagstiftning.

Harmoniserade standarder specificerar hur krav i EU-direktiv och EU-förordningar kan uppfyllas. När EU ger det europeiska standardiseringsorganet CEN i uppdrag att ta fram harmoniserade Europastandarder kallas detta för ”standardiseringsbegäran”. När EU-kommissionen hänvisar till en standard framtagna på detta sätt, innebär det att produkter som uppfyller kraven i standarden kan förutsättas uppfylla kraven i förordningen – ”presumtion om överensstämmelse”. Harmoniserade standarder är dock inte obligatoriska att följa.

Av utredningen framgår att när det gäller standardiseringsaktiviteter har ENISA, utöver förbättringar av diverse samarbeten, bland annat rekommenderat att standardiseringsorganisationer företrädesvis väljer att använda redan befintliga internationella standarder om sådana finns på det specifika området och att den internationella kommittén *ISO/IEC JTC1/SC 27 Information security, cybersecurity and privacy protection* bör betraktas som den första referensen för cybersäkerhetsstandardisering. I detta sammanhang bör även den europeiska standardiseringskommittén *CEN-CENELEC JTC 13 Cybersecurity and Data Protection* nämnas.¹ *CEN-CENELEC JTC 13* bedriver europeiskt standardiseringsarbete inom samma område som *ISO/IEC JTC1/SC 27*. Kommittén har möjlighet att selektera globala standarder som ska fastställas till europeisk standard. När detta sker innebär det att dessa standarder även måste fastställas till nationell standard i alla medlemsländer till CEN. Existerande standarder med samma syfte ska då dras tillbaka.

Utredningen lyfter fram standarder och standardiseringsorganisationerna som viktiga verktyg till stöd för cybersäkerhetscertifiering (se framförallt s. 85). SIS vill härvidlag påpeka att det är genom deltagande i SIS tekniska kommittéer som svenska organisationer kan vara med och påverka

¹ Se ENISA STANDARDISATION IN SUPPORT OF THE CYBERSECURITY CERTIFICATION Recommendations for European standardisation in relation to the Cybersecurity Act December 2019

innehållet i de standarder, såväl europeiska som internationella, som tas fram inom det aktuella området.

Av utredningen framgår att standardiseringsarbetet avseende informations säkerhet i huvudsak bedrivs inom ramen för SIS arbete kopplat till *ISO/IEC JTC 1/SC 27* (s. 116, fotnot nr. 29). SIS tekniska kommitté *SIS/TK 318 Informations säkerhet* bedriver standardiseringsarbete inom området informations säkerhet. *SIS/TK 318* speglar och deltar i de arbeten som sker inom *ISO/IEC JTC 1/SC 27* samt *CEN-CENELEC JTC 13*. Genom att delta i *SIS/TK 318* har svenska organisationer (såväl offentliga som privata) möjlighet att påverka de standarder som tas fram inom området.

Inom *SIS/TK 318* finns en undergrupp, *AG 31 Kravställning och verifiering*. Deltagarna i *AG 31* representerar Sverige i flera arbetsgrupper inom *ISO/IEC JTC 1/SC 27* och *CEN-CENELEC JTC 13*. På grund av bristfälligt deltagande *AG 31* för närvarande deltar vi i dagsläget dessvärre inte aktivt i det pågående standardiseringsarbetet inom *CEN-CENELEC* samt *ISO/IEC JTC 1/SC 27*. SIS välkomnar såväl svenska myndigheter som andra typer av organisationer att gå med i kommittén i syfte att kunna påverka och framföra svenska ståndpunkter i det europeiska och internationella standardiseringsarbetet.

SIS bedömer att kunskap om befintliga standarder till stöd för EU:s Cybersäkerhetsakt, liksom kännedom om utvecklingen och behoven av nya standarder, kommer vara avgörande för en god tillsyn enligt regelverket. Utredningen föreslår att Försvarets materielverk (FMV) ska bli nationell myndighet för cybersäkerhetscertifiering. FMV deltar i standardiseringsarbetet hos SIS, men har i dagsläget inget uttryckligt uppdrag, eller särskilda medel, för detta i sin instruktion eller sitt regleringsbrev, annat än ett återrapporteringskrav i enlighet med regeringens standardiseringsstrategi. SIS föreslår därför att regeringen överväger att, i enlighet med regeringens standardiseringsstrategi, genom myndighetsstyrning förtydliga ett uppdrag för FMV att delta i standardisering i FMV. Detsamma gäller andra myndigheter som bedöms vara av särskild vikt enligt utredningen.

SIS och projektledningen för *SIS/TK 318* står till förfogande vid eventuella frågor om standardisering och det svenska deltagandet.

Med vänlig hälsning

Annika Andreasen, VD
Svenska institutet för standarder

SIS är en ideell förening och ett svenskt standardiseringsorgan. SIS är utsedd av regeringen att representera Sverige i ISO och CEN.

SIS projektleder det svenska arbetet med att ta fram standarder och tillhandahåller och förvaltar standarder i Sverige. Vi finansierar vår verksamhet genom främst deltagaravgifter och försäljning av standarder.

SIS verkar för svenskt inflytande i internationell standardisering inom ISO och CEN, och för att standarder sprids och används i Sverige.

Hos SIS kan aktörer inom näringsliv, akademi, offentlig sektor och frivilligorganisationer ta initiativ till och utveckla standarder som främjar en god samhällsutveckling.