

		1 (4)
	Datum	
	Datum	Er referens/diarienummer
	2026-05-15	Fö2026/00576
Avsändarens kontaktperson	Mottagare	
elisabet.spross@sis.se	Försvarsdepartementet	

Svar på remiss: Försvarsdepartementet: EU:s cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten samt riktade ändringar i NIS 2-direktivet

Svenska institutet för standarder, SIS, tackar för möjligheten att lämna synpunkter på Europeiska kommissionens cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) samt riktade ändringar i NIS 2-direktivet (EU 2022/2555) KOM (2026)11, 13. SIS har tagit del av remissen och önskar lämna följande yttrande utifrån sitt uppdrag som nationellt standardiseringsorgan.

SIS yttrar sig i frågor som rör standardisering och hänvisning till standarder och tekniska specifikationer, genom SIS roll som nationellt standardiseringsorgan.

Bakgrund

Europeiska kommissionen föreslår i cybersäkerhetspaketet en revidering av cybersäkerhetsakten (EU 2019/881, bland annat genom en utvidgning av Europeiska unionens cybersäkerhetsbyrås (ENISA) mandat.

Enligt gällande ordning har ENISA haft en begränsad roll när det gäller tekniska specifikationer, främst att identifiera befintliga tekniska specifikationer i enlighet med bilaga II till förordning (EU) nr 1025/2012, i de fall harmoniserade standarder inte finns tillgängliga.

Genom förslaget till ny cybersäkerhetsakt ges ENISA i stället möjlighet att utveckla egna tekniska specifikationer för cybersäkerhetscertifierings ordningar. Ramarna för när, varför och under vilka förutsättningar sådana specifikationer ska tas fram klargörs dock endast översiktligt. Artikel 77 i förslaget anger vissa grunddrag för hur av ENISA-utvecklade tekniska specifikationer ska se ut, men utan närmare materiella eller processuella begränsningar.

SIS bedömning

SIS ser med viss oro på förslaget att utvidga rätten att utarbeta tekniska krav till organ utanför de europeiska standardiseringsorganisationerna (ESOs: dvs. CEN, CENELEC och ETSI).

Det europeiska standardiseringsystemet bygger på etablerade principer om transparens, öppenhet och konsensus. Dessa principer är centrala för att säkerställa teknikneutralitet, rättssäkerhet och bred acceptans i tillämpningen. När tekniska specifikationer får en normerande eller i praktiken bindande effekt inom unionsrätten är det särskilt viktigt att de tas fram inom tydligt reglerade processer.

SIS noterar att förslaget inte tydligt motiverar i vilka situationer harmoniserade standarder skulle vara otillräckliga, eller varför ENISA bör ges en självständig normgivande roll i dessa fall. Utan en snäv och tydlig avgränsning riskerar ENISA-utvecklade tekniska specifikationer skapa parallella spår.

SIS delar uppfattningen att exceptionella lösningar kan behövas i avsaknad av standarder, men anser att sådana lösningar måste omges av strikta undantagsfall.

SIS vill särskilt framhålla att stora delar av NIS2-direktivets krav, i synnerhet artikel 21 om cybersäkerhetsriskhantering, redan ligger i linje med etablerade internationella och europeiska standarder såsom SS-EN-ISO/IEC 27001:2022 och de säkerhetsåtgärder som beskrivs i SS-EN-ISO/IEC 27002:2022. Dessa standarder tillhandahåller ett riskbaserat, systematiskt och skalbart angreppssätt som redan används brett inom både offentlig och privat sektor i Sverige och övriga EU.

De delar som tillkommer genom NIS2 avser i huvudsak rapporteringsskyldigheter, tidsfrister och former för myndighetssamverkan, snarare än nya typer av tekniska eller organisatoriska säkerhetsåtgärder. Mot denna bakgrund finns en risk att av ENISA-utvecklade tekniska specifikationer skapar parallella efterlevnadsstrukturer i stället för att bygga vidare på befintligt standardiseringsarbete.

SIS rekommendationer

SIS rekommenderar att bestämmelserna om ENISA-utvecklade tekniska specifikationer tydligare ramar in och begränsas, i syfte att värna det europeiska standardiseringssystemets roll.

1. ENISA:s möjlighet att utveckla tekniska specifikationer begränsas till undantagsfall, där det tydligt kan konstateras att harmoniserade standarder saknas och inte kan tas fram inom rimlig tid.
2. Regelverket för ENISA:s tekniska specifikationer utformas i nära analogi med EU-rättens regler om gemensamma specifikationer, såsom de används i annan produkt- och säkerhetslagstiftning (exempelvis Cybersäkerhetsförordning innehåller Artikel 27, p 2.).
3. Som förebild bör särskilt övervägas den reglering av gemensamma specifikationer som återfinns i leksaksförordningens bestämmelser, vilka också har förordats av rådet och kännetecknas av:
 - tydlig subsidiaritet i förhållande till standarder,
 - krav på exceptionella omständigheter, samt
 - transparens och möjlighet till deltagande för berörda aktörer.
4. Det i rättsakten tydligt anges att harmoniserade europeiska standarder ska vara förstahandsalternativet, och att ENISA-utvecklade tekniska specifikationer inte får ersätta eller konkurrera med pågående standardiseringsarbete inom ESO:erna. Särskilt bör SS-EN-ISO/IEC 27001:2022 och SS-EN-ISO/IEC 27002:2022 erkännas som centrala standarder för cybersäkerhetsriskhantering.

En sådan utformning skulle enligt SIS bidra till en bättre balans mellan behovet av effektiv cybersäkerhetsreglering och långsiktig tillit till det europeiska standardiseringssystemet.

Begränsningar av deltagande i standardisering

Utöver ovanstående synpunkter på ENISA vill SIS även kommentera de föreslagna begränsningarna av deltagande i europeisk standardisering enligt artikel 100 (4). Även om säkerhetsskäl i vissa fall kan motivera riktade åtgärder, framstår definitionen av högriskleverantörer som oklar. Samtidigt är det centralt att öppenhet och transparens i standardiseringsprocessen fortsatt säkerställs. Europeisk standardisering bygger på bred och inkluderande medverkan samt den nationella delegationsprincipen. Eventuella begränsningar av deltagande bör därför utformas restriktivt och ske i nära dialog med de europeiska standardiseringsorganisationerna för att inte undergräva förtroendet för systemet.

Allmänt om standardisering och dess samband med EU-lagstiftning

SIS anser att det finns tydliga fördelar med att använda den formella standardiseringen för att uppnå de mål som sätts upp i förslaget. En av fördelarna med den formella standardiseringen och användningen av harmoniserade standarder är att den kan fungera som ett komplement till lagstiftningen i situationer där lagstiftaren av olika skäl inte ansett det lämpligt att reglera eller då man inte vill reglera krav i detalj.

Harmoniserade europeiska standarder är standarder som tas fram på uppdrag av EU-kommissionen för att stödja EU-lagstiftning eller andra politiska initiativ. Detta sker genom att EU-kommissionen begär relevanta standarder från de europeiska standardiseringsorganisationerna (CEN/Cenelec) som stöd för regelefterlevnad (så kallad standardiseringsbegäran).

Harmoniserade standarder citerade i Europeiska Unionens Officiella Tidning (EUT) ger en presumtion om överensstämmelse med unionens rättsakter.

Harmoniserade standarder utvecklas genom samverkan mellan kommissionen, standardiseringsorganisationerna, industrin, och övriga intressenter, och är en central förutsättning för den inre marknadens funktion och Europas konkurrenskraft.

Avslutande kommentar

SIS betonar att myndighetsmedverkan i standardiseringen är avgörande för att säkerställa att cybersäkerhetspaketet och cybersäkerhetsakten får önskvärd effekt. Inom många standardiseringsområden har SIS ett brett deltagande men vi ser alltid behov av ökad representation från myndigheter. Engagemang i standardisering ger bättre insyn, påverkan och stärker både samhällsutveckling och konkurrenskraft. Därtill bidrar en ökad myndighetsmedverkan till att standardiseringsarbetet får tillgång till viktig kompetens, nya perspektiv och nödvändiga ekonomiska resurser för att tillvarata svenska intressen i det internationella arbetet.

SIS uppmuntrar till att:

Frågeställaren engagerar sig i standardiseringsarbetet och kontakter SIS för mer information om befintligt arbete samt för att påbörja standardisering inom nya områden.

Vi ger gärna ytterligare information och svarar gärna på frågor om existerande standarder och pågående standardiseringsarbete.

Med vänlig hälsning,

Sarah Sim,
Standardiseringschef
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.

Vid certifiering, validering och verifiering blir användning av standarder en del av den internationella kvalitetsinfrastrukturen som bl.a. sker genom de officiella ackrediteringsorganen, exempelvis Swedac i Sverige.

Standardiseringskommittéer som drivs gemensamt mellan ISO respektive CEN och de internationella organisationerna för elektroteknisk standardisering IEC respektive Cenelec bevakas av både SIS och SEK Svensk Elstandard som är utsedd av regeringen att ansvara för all standardisering inom det elektrotekniska området i Sverige och är svensk nationalkommitté inom IEC och Cenelec.