

Avdelningen för verksamhetsstöd  
Tomas Hedlund  
tomas.hedlund@socialstyrelsen.se

Regeringskansliet  
Justitiedepartementet  
103 33 STOCKHOLM

## Socialstyrelsens yttrande över betänkandet Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten (SOU 2015:23)

Socialstyrelsen anser att det är angeläget att skapa en gemensam syn på en lägsta nivå av informationssäkerhet i staten och samtidigt höja lägstanivån. Socialstyrelsen tillstyrker införandet av strategi och ett myndighetsråd men avstyrker utformningen av paragrafer 6, 8, 11, 16 och 19 i den föreslagna förordningen.

### **Förslag till förordning för statliga myndigheters informationssäkerhet**

6 § Det är oklart hur man definierar begreppet myndighetens ledning. Begreppet verkar definieras annorlunda än i myndighetsförordningen (2007:515).

8 § Det bör tydliggöras när bristande informationssäkerhet kan medföra en betydande försämring av myndigheters förmåga att bedriva sin verksamhet, och vad som i sammanhanget avses med betydande försämring.

Vidare saknas författningsförslag till; förslaget om kravställning vid upphandling i avsnitt 9.3.1 och förslag till tidskala för tidsangivelser i avsnitt 9.4.1. Socialstyrelsen har i dessa fall inte kunnat ta närmare ställning till förslagen.

Socialstyrelsen noterar också att utredningen i avsnitt 9.4.1 pekar på att en närmare analys av de legala frågorna kring utformning och användning av sensorsystem behöver göras. Samtidigt föreslås i 11 § förslaget till förordning att myndigheter som har ett särskilt ansvar för krisberedskap ska uppfylla särskilda krav på informationssäkerhet rörande användning av sensorsystem för it-incidentifiering. Socialstyrelsen avstyrker detta förslag i avvaktan på att en närmare analys av de legala frågorna görs.

Socialstyrelsen anser vidare att det är av vikt att samma begrepp och definitioner används i de regelverk som är under framtagande t ex En ny säkerhetsskyddslag (SOU 2015:25) och Förslag till Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (Dnr 2014-6391).

Förslagsvis kan terminologi i SIS teknisk rapport 50 användas. Definitionen av begreppet informationssäkerhet ("förmågan att upprätthålla") överensstämmer inte heller med praxis och svensk standard. Begreppet it-incident bör inte användas när det som avses antingen är it-säkerhetsincident eller informations-säkerhetsincident. Därtill behövs en definition av valt begrepp. Myndigheterna bör arbeta utifrån ett ledningssystem baserat på svensk standard för informationssäkerhet dvs. SIS 27001-standarden.

16 § Säkra it-produkter är ett olyckligt begrepp och inte entydigt. Det bör finnas möjlighet för varje myndighet att bedöma t.ex. vilka it-produkter som är rimliga att använda ur verksamhets- och kostnadsperspektiv för att få en balanserad skyddsnivå. Vidare är det oklart hur säkra it-produkter ska hanteras upphandlingsmässigt.

19 § MSB får i och med tillsynen dubbla roller då MSB dels ska leda det stödjande Myndighetsrådet och dels utöva tillsyn över statliga myndighetens informationssäkerhetsarbete. Det är därför viktigt att de olika rollerna klargörs och hur tillsynen ska utövas i praktiken.

## **Synpunkter på konsekvensanalys (kapitel 10)**

Den samlade ambitionshöjningen med ett ökat ansvar för det praktiska säkerhetsarbetet, utvecklad internrevision och obligatorisk it-incidentrapportering kommer att medföra ett ökat resursbehov för de enskilda myndigheterna. Socialstyrelsen vill också lyfta fram att förslagen medför ett utökat behov av praktiskt stöd åt myndigheterna och att stödet bör tas fram skyndsamt.

Exempel på arbetsuppgifter som för flera myndigheter kommer att medföra ökade resursbehov är anslutning, drift och förvaltning av ny obligatorisk SGSI-anslutning samt den nya obligatoriska incidentrapporteringen

## **Synpunkter på den föreslagna strategin och åtgärder (bilaga 5)**

Socialstyrelsen är i huvudsak positiv till strategin med tillhörande åtgärder. Lika viktigt som en tydlig styrning och stöd från MSB är stödet myndigheter emellan. Socialstyrelsen bedömer att betydande effektivitetsvinster i arbete kan uppnås genom att myndigheterna lär av varandra genom att utbyta metoder och erfarenheter. Detta eftersom myndigheternas arbetssätt i många delar kommer att

vara lika eller snarlika. Det saknas dock förslag som (administrativt och tekniskt) underlättar ett sådant samarbete.

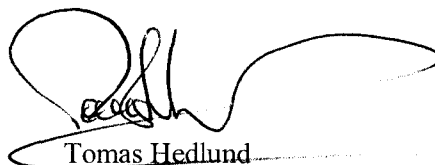
Den föreslagna styrmodellen bör baseras på och vara helt i linje med svensk och internationell standard och styrmodell för informationssäkerhet (ISO 27000-serien) i likhet med MSB:s föreskrift om myndigheters informationssäkerhet (2009:10).

Beslut i detta ärende har fattats av generaldirektör Lars-Erik Holm. I den slutliga handläggningen har ställföreträdande generaldirektör Taina Bäckström, avdelningschef Erik Höglund, biträdande chefsjurist Lars Hobert och stabschef Annika Nordlander Finn deltagit. Föredragande har varit avdelningschef Tomas Hedlund.

SOCIALSTYRELSEN



Lars-Erik Holm



Tomas Hedlund