PENSIONS MYNDIGHETEN

Remissyttrande

2015-09-09

Dnr/Ref. VER 2015-186

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad

Dnr 2014-6391

MSB FS nya föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet

Inledningen och sammanfattning
Informationssäkerheten i de statliga myndigheterna behöver stärkas och Pensionsmyndigheten ser positivt på att MSB uppdaterar föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet.

Dock anser vi att tidpunkten för uppdateringen inte är lämplig och avstyrker förslaget att de ska träda i kraft den 1 januari 2016. Det sker just nu andra pågående utredningar inom informationssäkerhet som påverkar de statliga myndigheternas informationssäkerhetarbete, främst SOU 2015:23 Informations- och cybersäkerhet i Sverige och SOU 2015:25 En ny säkerhetsskyddslag. Det är viktigt att MSB:s förslag till föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet stämmer överens med de förslag som presenteras i de olika utredningarna, vilket vi i dagsläget anser att de inte gör fullt ut. När ovanstående utredningar är hanterade och det står klart vilka nya författningskrav m.m. de resulterar i anser vi att tidpunkten är lämplig för MSB att uppdatera sina föreskrifter och allmänna råd. Detta för att säkerställa att föreskrifterna och de allmänna råden både teoretiskt och praktiskt hanterbart hänger ihop med de övriga föreskrifterna och kraven.

Vi är kritiska till några av förslagen i MSB:s föreskrift och allmänna råd, främst att det inte längre föreskrivs användning av de svenska standarderna SS-ISO/IEC 27001 och 27002 för ledningssystem för informationssäkerhet, samt även att det ställs ett uttryckligt krav på att kartlägga verksamhetsprocesser.
Genom att använda standarderna SS-ISO/IEC 27001 och 27002 anser vi att det skapas förtroende och att samverkan underlättas mellan statliga myndigheter och kommersiella aktörer, både inom Sverige och internationellt. Standarderna ger även möjlighet att anpassa arbetet med informationssäkerhet till den egna organisationen. Avseende det uttryckliga kravet på att kartlägga verksamhetsprocesser anser vi att det finns olika adekvata metoder för att identifiera myndighetens egna krav på informationssäkerhet och att den enskilda myndigheten själv ska avgöra vilken metod som är mest effektiv och bäst tillämpbar.

Vi anser även att konsekvensutredningen inte tillräckligt analyserar konsekvenserna av de föreslagna förändringarna för de enskilda statliga myndigheterna.

Att bedriva ett systematiskt informationssäkerhetsarbete är resurs- och kompetenskrävande och det finns ett stort behov av erfarenhetsbaserat praktiskt stöd. Vi önskar att MSB kan ge ett utökat stöd och samordning, förslagsvis genom det myndighetsråd som föreslås i SOU 2015:23. Exempelvis skulle MSB kunna dela med sig av egna erfarenheter från införandet av föreskriften i den egna organisationen.

Pensionsmyndigheten	Telefon	Fax	E-post	Org.nr
Box 38190 100 64 Stockholm	0771-771 771	08-658 13 00	registrator@pensionsmyndigheten.se	202100-6255

Pensionsmyndigheten har följande synpunkter på de enskilda föreskrifterna.

2 §
Vi anser att det andra stycket är otydligt och behöver förtydligas avseende ansvar för informationssäkerhet i de fall en myndighets informationshantering eller informationssäkerhetsarbete helt eller delvis administreras av en annan myndighet.

5 §
Vi anser att föreskriften ska ange att myndigheterna ska tillämpa ett ledningssystem för informationssäkerhet baserat på standarderna SS-ISO/IEC 27001 och 27002. Det skapar förtroende och underlättar samverkan mellan statliga myndigheter och kommersiella aktörer, både inom Sverige och internationellt. Standarderna ger även möjlighet att anpassa arbetet med informationssäkerhet till den egna organisationen.
Vi föreslår också en ny formulering av den sista meningen i paragrafen:
”Det ska säkerställas att det sker en adekvat resurstilldelning för informations-säkerhetsarbetet och att myndighetens ledning löpande informerar sig om arbetet med informationssäkerhet. Myndigheten ska minst en gång per år följa upp och utvärdera informationssäkerhetsarbetet på myndigheten.”

6 §
Det är önskvärt att paragrafen förtydligas så att även mål för informationssäkerhetsarbetet ingår i ledningssystemet.

8 §
Vi anser inte att det ska ställas ett uttryckligt krav på att kartlägga verksamhetsprocesser. Vi anser att det finns olika adekvata metoder för att identifiera myndighetens egna krav på informationssäkerhet och att den enskilda myndigheten själv ska avgöra vilken metod som är mest effektiv och bäst tillämpbar. Vidare anser vi att rollen informationsägare bör beskrivas ytterligare.
Vi föreslår att paragrafen får följande lydelse. *”Myndigheten ska identifiera krav på informationssäkerhet med stöd av den modell eller metod som myndigheten beslutat.”*

10 §
Vi önskar ett förtydligande om klassning av information ska ske enligt en modell som myndigheten själva beslutar eller om MSB:s ”Modell för klassificering av information” ska användas. Vi föreslår också en ny formulering av punkt 3:
”3 utifrån informationsklassningens resultat och genomförd riskanalys identifiera och införa åtgärder (skyddsnivå) som motsvarar informationens krav på skydd,”

11 §
Det är viktigt att det tydliggörs att roller med tillhörande ansvar och befogenheter även ska definieras för incidenthantering. Vidare behöver begreppen som berör incidenthantering stämma bättre överens mellan MSB:s förslag till föreskrifter där begreppet ”informationssäkerhetsincidenter” används, medan det i SOU 2015:23 istället är begreppet ”IT-incidenter” som används och i SOU 2015:25 är de tre begreppen ”incident, säkerhetsincident och IT-incident” som används.

Vi har följande synpunkter på de allmänna råden om statliga myndigheters informationssäkerhet

Kommentar till 7 §
Vi anser att formuleringen *”informationssäkerhetspolicy och andra styrande dokument utgör systemdokumentation av LIS”* felaktigt kan leda tanken till krav om system-dokumentation som finns i bokföringslagen eller till systemdokumentation för IT-system. Vi föreslår istället denna formulering:
”Informationssäkerhetspolicyn och tillhörande styrande dokument ska beskriva mål och säkerhetsåtgärder för informationssäkerhet, roller och ansvarsfördelning för informationssäkerhet samt definition och omfattning av ledningssystemet.”

Kommentar till 8 §
Om syftet med skrivningen är att underlätta för verksamheten att ställa krav på informationssäkerhet bör myndigheterna själva besluta om vilken metod som är bäst lämpad utifrån den egna organisationens och verksamhetens förutsättningar.

Kommentar till 11 §
När det gäller det första stycket önskar vi att vikten av att dra lärdomar från inträffande incidenter och att anpassa skyddsnivåer och säkerhetsåtgärder efter dessa tydliggörs.

Vi har följande synpunkter på konsekvensutredningen

Vi anser att konsekvensutredningen inte tillräckligt analyserar konsekvenserna av de föreslagna förändringarna för de enskilda statliga myndigheterna. Den nuvarande konsekvensbeskrivningen är istället mer fokuserad på att förklara vilka ändringar som MSB genomför i föreskrifterna och de allmänna råden samt bakgrund och motivering till de enskilda ändringarna.

Den enda kostnadsökning som redovisas för de enskilda myndigheterna är en kortsiktig kostnadsökning relaterat till utbildning och övning.
Vi anser att konsekvensutredningen är bristfällig och vill exempelvis att konsekvensen av 8 § (kartläggning av verksamhetsprocesser) i föreskriften utreds närmare. Ett sådant krav är enligt vår erfarenhet kostsamt då det kräver personella resurser för att genomföra kartläggningen och för att hålla den aktuell och uppdaterad över tid.

Vi håller inte med om resonemanget avseende vid vilken tidpunkt föreskrifterna ska träda ikraft. Vi anser att MSB:s förslag till föreskrifter och allmänna råd i större utsträckning måste stämma överens med resultatet från utredningarna SOU 2015:23 och SOU 2015:25.

Vidare anges att de nya föreskrifterna och allmänna råden skulle motsvara de statliga myndigheternas utökade behov av stöd till följd av konsekvenserna från SOU 2015:23 och SOU 2015:25. Vi anser att detta inte går att avgöra i dagsläget innan det är klarlagt vad de två ovanstående utredningarna fullt ut resulterar i för de enskilda myndigheterna. Till detta kommer att dessa betänkanden för närvarande är under remissbehandling och att det alltså är osäkert om och hur det kommer att genomföras. Därför bör MSB avvakta med att ge ut nya föreskrifter och allmänna råd till dess att det står klart vilka krav m.m. utredningarna resulterar i för de enskilda myndigheterna. Först då kan MSB anpassa sina föreskrifter och allmänna råd så att de ger det eventuella utökade stöd som myndigheterna efterfrågar.

Att bedriva ett systematiskt informationssäkerhetsarbete är resurs- och kompetenskrävande och det finns ett stort behov av erfarenhetsbaserat praktiskt stöd. Vi önskar att MSB kan ge ett utökat stöd och samordning, förslagsvis genom det myndighetsråd som föreslås i SOU 2015:23. Exempelvis skulle MSB kunna dela med sig av egna erfarenheter från införandet av föreskriften i den egna organisationen.

Detta yttrande har beslutats av generaldirektör Katrin Westling Palm efter föredragning av informationssäkerhetsansvarig Ingrid Holmström. I den slutliga handläggningen har även avdelningschef, säkerhetschef och säkerhetsskyddschef Henrik Engström deltagit.

Katrin Westling Palm

Ingrid Holmström