Riksdagens protokoll 2017/18:9

Fredagen den 22 september

Kl. 09.00–09.24

---

§ 1 Avsägelse

Förste vice talmannen meddelade att *Adnan Dibrani* (S) avsagt sig uppdraget som ledamot i skatteutskottet.

Kammaren biföll denna avsägelse.

§ 2 Anmälan om kompletteringsval

Förste vice talmannen meddelade att Socialdemokraternas riksdagsgrupp anmält Anna Johansson som ledamot i skatteutskottet och ClasGöran Carlsson som suppleant i civilutskottet.

Förste vice talmannen förklarade valda till

ledamot i skatteutskottet
Anna Johansson (S)

suppleant i civilutskottet
ClasGöran Carlsson (S)

§ 3 Anmälan om subsidiaritetsprövning

Förste vice talmannen anmälde att utdrag ur prot. 2017/18:1 för torsdagen den 14 september i ärende om subsidiaritetsprövning av EU-förslag hade kommit in från justitieutskottet.

§ 4 Ärende för hänvisning till utskott

Följande dokument hänvisades till utskott:
Proposition
2017/18:17 till utbildningsutskottet

§ 5 Svar på interpellation 2016/17:548 om skyddet mot cyberangrepp

Anf. 1 Justitie- och inrikesminister MORGAN JOHANSSON (S):

Herr talman! Pål Jonson har frågat mig om jag delar uppfattningen att det finns mycket allvarliga brister i skyddet mot cyberangrepp hos svenska myndigheter, vilka nya åtgärder jag och regeringen i så fall avser att vidta i ljuset av de omfattande cyberangreppen och slutsatserna i årsrapporterna från Säpo, FRA och Must samt när jag och regeringen avser att presentera den nationella strategin för samhällets informations- och cybersäkerhet.

Det finns ett stort behov av att utveckla informationssäkerheten i Sverige. Sedan regeringen tillträdde har därför en rad åtgärder vidtagits. Exempelvis beslutade regeringen i december 2015 om obligatorisk it-incidentrapportering för statliga myndigheter. Sedan den 1 april 2016 är statliga myndigheter skyldiga att redovisa it-incidenter som de drabbas av.

Myndigheten för samhällsskydd och beredskap, MSB, har tillförts ökade resurser för att stärka samhällets motståndskraft mot it-angrepp. I vårändringsbudgeten för 2017 tillförde regeringen 10 miljoner kronor till MSB för att förstärka arbetet med informationssäkerhet och psykologiskt försvar. I budgetpropositionen 2018 fyrfaldigar och permanentar regeringen ökningen av medel utifrån en överenskommelse mellan regeringen, Moderaterna och Centerpartiet.

Nästa år kommer dessutom ännu fler leverantörer av samhällsviktiga och digitala tjänster att bli skyldiga att rapportera allvarliga it-incidenter och vidta andra säkerhetsåtgärder. Denna skyldighet träder i kraft när EU:s direktiv om åtgärder för en hög gemensam nivå av säkerhet i nätverk och informationssystem, NIS-direktivet, har genomförts.

Det pågår också ett viktigt arbete med att modernisera och skärpa säkerhetsskyddslagen. Här kan också nämnas Utredningen om vissa säkerhetsskyddsfrågor som ska föreslå åtgärder för att förbättra skyddet för de allra mest skyddsvärda verksamheterna. Utredaren ska bland annat föreslå förebyggande åtgärder för att säkerhetsskyddade uppgifter, eller säkerhetskänslig verksamhet, inte ska utsättas för risker i samband med utkontraktering, upplåtelse och överlåtelse av sådan verksamhet. I uppdraget ingår även att föreslå ett system med sanktioner i säkerhetsskyddslagen.

Försvarsmakten har regeringens uppdrag att, med stöd av Försvarets radioanstalt, FRA, och eventuellt övriga berörda myndigheter, utveckla och förstärka Sveriges cyberförsvar. För de mest skyddsvärda verksamheterna tillhandahåller FRA ett tekniskt detekterings- och varningssystem, TDV. TDV är en verksamhet som fick utökade resurser i vårändringsbudgeten 2017 och genom regeringens förslag om permanenta förstärkningar av FRA:s verksamhet från och med 2018.

Slutligen uppdrogs Säkerhetspolisen och FRA i april i år att redovisa vilka ytterligare åtgärder som kan vidtas för att motverka de allvarligaste hoten mot de mest skyddsvärda verksamheterna i Sverige. Redovisningen har lämnats, och mot bakgrund av den föreslår regeringen ytterligare förstärkning av myndigheternas arbete med informations- och cybersäkerhet.

Exemplen ovan illustrerar vikten av samverkan och en gemensam riktning. Den 29 juni 2017 presenterade därför regeringen en ny nationell strategi för hur informations- och cybersäkerheten i Sverige ska utvecklas och stärkas. Strategin sätter upp målsättningar inom sex prioriterade områden, och regeringen har redan påbörjat implementeringen genom att samma dag besluta om fyra regeringsuppdrag med koppling till strategin.

Jag kommer att fortsätta att noga följa arbetet med att stärka samhällets informations- och cybersäkerhet och vidta ytterligare åtgärder när det behövs.

Anf. 2 PÅL JONSON (M):

Herr talman! Tack, justitieministern, för svaret på min interpellation! Jag vill inledningsvis säga att jag har förståelse för att regeringsombildning och sommaruppehåll fördröjer interpellationssvar men konstaterar att den här interpellationen ställdes för fyra månader sedan. Vid den tidpunkten kände regeringen till det säkerhetshaveri som hade ägt rum på Transportstyrelsen. Det gjorde dock inte vi inom oppositionen när jag ställde den här interpellationen.

Haveriet inom Transportstyrelsen har naturligtvis pekat på många av de problem som även Must, FRA och Säpo tar upp i sina årsrapporter när det kommer till säkerhetsskyddet i Sverige. De årsrapporterna pekar rätt så entydigt på att det finns stora brister i säkerhetsmedvetandet hos svenska myndigheter, bland annat kopplat till cybersäkerhet. Det finns en begränsad förmåga hos svenska myndigheter att göra analyser av vad det är som är skyddsvärd verksamhet. Dessa myndigheter pekar också på att de finns brister i Sverige när det gäller den it-relaterade infrastrukturen hos svenska myndigheter.

Det framstår alltså utan tvekan som om det har vuxit fram någon form av säkerhetskultur i Sverige som är bristande när det kommer till cybersäkerhet, och jag tycker att detta är speciellt allvarligt för de myndigheter som har ett bevakningsansvar inom totalförsvaret, framför allt i ljuset av det försämrade säkerhetspolitiska omvärldsläget.

Ministern är ju mycket väl bekant med den granskning som Riksrevisionen gjorde av it-säkerheten på nio svenska myndigheter och som faktiskt till del var dräpande i sin kritik gällande dessa myndigheters förmåga att hantera cyberangrepp. Vi har ju till och med inom polisen sett fall där det verkar finnas en bristande säkerhetskultur, mot bakgrund av att rikspolischefen var i justitieutskottet så sent som i går och redogjorde för varför man gjort en avträdelse från säkerhetsskyddsförordningen.

Ett annat område som också tar spjärn i de brister som finns när det gäller cybersäkerhet är att den it-relaterade brottsligheten i Sverige har ökat med över 900 procent under det senaste årtiondet. Utredningsresultaten från polisen på detta område ser bedrövliga ut, och detta är den snabbast växande brottsligheten som vi har att hantera i Sverige.

Även i en internationell jämförelse är det uppenbart att Sverige inte ligger väl till när det gäller cybersäkerhet. På World Economic Forum i Davos för två år presenterades en mätning som pekade på att Sverige är världens tredje mest digitaliserade och uppkopplade land, medan vi i den mätningen inte ens nådde topp 50 gällande cybersäkerhet.

Nu vet jag att det har skett framsteg de senaste två åren, men det råder ingen tvekan om att regeringen har ett grannlaga arbete framför sig för att höja cybersäkerheten.

Jag vill också vara klar med att det faller en skugga även över alliansregeringen. Vi skulle ha gjort mer för att höja säkerhetsskyddet för cybersäkerhet. Men nu är det regeringen som äger frågan, och det är därför som jag vill se ledarskap från regeringen.

Avslutningsvis, herr talman, har jag två kommentarer till ministerns svar. Ministern säger att det finns ett behov av att höja informationssäkerheten i Sverige. Jag delar den analysen, men jag vet också att ett skäl till att vi gör det kanske inte är så mycket för de hot och risker som finns utan för att EU nu ställer nya krav på oss genom NIS-direktivet.

Jag vill därför veta om ministern delar Musts, FRA:s och Säpos bedömning att det finns mycket stora och allvarliga brister i skyddet mot cyberangrepp. Det är viktigt för oss i oppositionen att veta om man delar de egna myndigheternas och oppositionens analys eller inte.

När det gäller incidentrapportering är det bra att regeringen har genomfört detta och att det är obligatoriskt. Underrapporteringen är mycket stor på detta område, och det behöver man hantera. FRA gick i januari ut och sa att Sverige utsatts för 10 000 statssanktionerade angrepp.

Anf. 3 Justitie- och inrikesminister MORGAN JOHANSSON (S):

Herr talman! Det är riktigt som Pål Jonson säger att det har dragit ut på tiden att besvara den här interpellationen, eftersom sommaruppehållet kom emellan. Å andra sidan kan vi redovisa ytterligare saker som vi har gjort, bland annat den strategi som Pål Jonson efterfrågar i sin interpellation. Det fattade vi beslut om under sommaren, så det har vi genomfört.

Jag uppskattar också att Pål Jonson markerar att det har skett framsteg under de här två åren och att det är ett gemensamt politiskt ansvar att se till att vi ökar cybersäkerheten i landet totalt sett.

Om vi går tillbaka ser vi att det har skett ett antal granskningar. Riksrevisionen gjorde 2014 en granskning av den förra regeringens informationssäkerhetsarbete och kom då fram till att det fanns brister när det gäller styrningen av myndigheternas informationsarbete. Man lämnade även en rad rekommendationer till den tillträdande regeringen, vilket vi nu tar hand om. Vid det tillfället reagerade Riksrevisionen också på att den tidigare regeringen inte hade agerat tillräckligt trots att de första bristerna påtalades för ett antal år sedan, nästan tio år sedan i det här läget.

När regeringen tillträdde 2014 drog vi igång ett arbete för att stärka skyddet mot cyberangrepp. De hoten kan vara av olika slag och dignitet. Det kan vara allt från tonårshackare som bara vill testa systemen till kriminella som vill åt information för att tjäna pengar eller stjäla pengar, till terrorister som vill slå ut delar av samhällets it-infrastruktur bara för att skapa oreda och kaos eller, som allra värst, främmande makt som vill nästla sig in i våra informationssystem för att komma åt det som är vår mest skyddsvärda information, det vill säga den typ av information som har bäring på rikets säkerhet.

Angriparna kan vara av många olika slag, motiven ännu fler och metoderna oräkneliga. Att skydda sig är därför både svårt och komplext men kan visa sig vara avgörande i en krissituation. Regeringen har därför vidtagit en rad åtgärder för att höja vår beredskap, för att stärka kompetensen och för att öka vår förmåga att stå emot cyberangrepp av olika slag.

Riksrevisionen krävde till exempel den obligatoriska it-incidentrapporteringen. Den finns nu på plats. Vi fattade beslut om den 2015, och 2016 kom den på plats. Den behövs för att kunna bedöma hoten och vår sårbarhet. Då måste vi få löpande information om olika försök att ta sig in i och manipulera våra system.

Nu finns en ordning som innebär att alla statliga myndigheter skyndsamt ska rapportera alla allvarliga it-incidenter. De ska rapportera antingen till MSB, till Säpo eller till Försvarsmakten beroende på vilken typ av incident det handlar om. År 2016, förra året, tog MSB emot 214 sådana it-incidentrapporter från 77 myndigheter. 12 av dem polisanmäldes.

För första gången finns nu en mer samlad bild av vad Sverige utsätts för, även om det naturligtvis ändå finns, som Pål Jonson påpekar, ett stort mörkertal. Det handlar om att fortsätta att jobba med det verktyget för att få in mer och mer information av det slaget.

Vidare ökar regeringen anslagen kraftigt till de myndigheter som har en central roll för it-säkerheten. Det är först och främst MSB, som fick 10 miljoner i år. Vi bygger ut med ytterligare pengar och fyrfaldigar stödet till 40 miljoner kronor från nästa år. FRA får ytterligare 20 miljoner nästa år för sitt viktiga arbete. Säkerhetspolisen får också ytterligare 40 miljoner. Sammanlagt är det från nästa år ytterligare 100 miljoner kronor till dessa centrala myndigheter för att arbeta för att öka cybersäkerheten.

Anf. 4 PÅL JONSON (M):

Herr talman! Låt mig först ge en kort kommentar om it-incidentrapporteringen. Det var bara tre av anmälningarna som riktades till Säpo, alltså kopplade till säkerhetsskydd. Det var ingen anmälning som gick till Försvarsmakten. I ljuset av FRA:s bedömning att Sverige utsätts för så många statssanktionerade angrepp är det helt uppenbart att mörkertalet är betydande. Jag skulle gärna vilja veta om ministern avser att vidta några åtgärder för att komma till rätta med detta mörkertal. Lägesbilden är, precis som ministern säger, mycket viktig.

Jag skulle också vilja ta fasta på regeringens it- och säkerhetsstrategi, som regeringen har presenterat. Regeringen har tagit rätt god tid på sig att presentera strategin med tanke på att den är ett år försenad. Jag konstaterar att det är svårt att skriva sådana samlingsdokument, och jag vet att det finns bättre och sämre strategier som har presenterats. Vägen till framgång går genom att våga prioritera och vara tydlig i strategierna.

En strategi ska normalt innehålla tre M, nämligen mål, medel och metod. Den strategi som regeringen har presenterat är utan tvivel rik på mål. Den utgår från de tre målen i den nationella säkerhetsstrategin. Det är bland annat digitaliseringsmålet, det vill säga att Sverige ska vara bäst i världen när det kommer till digitalisering. Det målet har sex nedbrutna it-mål och 54 delmål. Det blir faktiskt 68 målsättningar på 32 sidor i det dokumentet.

En välvillig tolkning är att regeringen har höga ambitioner. Men problemet när så mycket fokus läggs på mål är att de andra två frågorna, de riktigt intressanta i en strategi, nämligen hur de ska förverkligas och vilka medel som ska avsättas, visar att strategin i det avseendet tyvärr har stora brister.

Jag skulle vilja ta upp tre sådana brister som jag har identifierat.

För det första är jag verkligen överraskad att strategin är så kortfattad när det kommer till upphandling och outsourcing, trots att strategin skrevs med insikten i Regeringskansliet om det haveri som hade ägt rum på Transportstyrelsen och med insikten om att Säpo redan 2012 varnade för risker och problem med outsourcing. Den utredning som låg till grund för strategin, skriven av Erik Wennerström, sa att vi måste våga använda lagen om upphandling för försvars- och säkerhetsprodukter och inte bara lagen om offentlig upphandling. Det var själva cloun i utredningen. Ändå hanteras upphandling mycket rapsodiskt i strategin. Det är en brist. Det är verkligen överraskande i ljuset av vad regeringen då visste om Transportstyrelsen och vad vi vet i dag.

För det andra vill jag ta fasta på att strategin lyfter fram behovet av samverkan med privata näringslivet. Det är helt rätt. All teknikutveckling i dag sker inom privata företag. Det behövs dialog och samband. Men regeringen specificerar inte hur samverkan ska ske vid sidan av de forum som MSB har. Det är en bra verksamhet men också en mycket avgränsad verksamhet.

För det tredje, och det är stort, är regeringen inte tydlig i organisationsfrågan. Det är fortfarande fyra ministrar och sex myndigheter som arbetar med digitalisering och i någon mån cyberstrategi. Det utgör en brist att man inte är tydlig.

Herr talman! Det står ingenting i strategin om Regeringskansliets egen organisation i fråga om cybersäkerhetsfrågor. Vi vet nu att det inte gick bra för regeringen och Regeringskansliet att hantera Transportstyrelsen. Avser ministern att vidta några åtgärder där som inte framgår av strategin?

Anf. 5 Justitie- och inrikesminister MORGAN JOHANSSON (S):

Herr talman! Nu finns ett system för it-incidentrapporteringar på plats. Det kan säkert finnas ett mörkertal, som jag var inne på tidigare, men det här är första året. För att minska mörkertalet måste vi se till att kompetensnivån höjs och att det finns större beredskap och vaksamhet när den typen av incidenter inträffar.

Det är därför som regeringen är beredd att sätta av pengar. Jag tog i mitt tidigare anförande upp att vi nu fyrfaldigar anslaget till MSB från årets 10 miljoner till 40 miljoner nästa år. Om man lägger ihop de pengar som nu sätts av till dessa ändamål, där även andra myndigheter förstärks nästa år, kan man se att det är ett riktigt lyft på området.

MSB, FRA och Säpo, våra tre centrala myndigheter på området, får från nästa år, 2018, riktade pengar, över 100 miljoner kronor ytterligare för att arbeta med bland annat dessa frågor. År 2019 får de 150 miljoner kronor ytterligare, och år 2020 får de över 180 miljoner kronor ytterligare. Strategin handlar inte bara om mål, utan vi förser de myndigheter som behöver pengar till dessa frågor med just de resurser de behöver.

Sedan var det frågan om it-incidentrapportering. Jag kan tillägga att när NIS-direktivet implementeras, vilket kommer att ske under våren, utvidgas skyldigheten att rapportera in it-incidenter inte bara till de statliga myndigheterna utan också till leverantörer och därmed en stor andel i den privata sektorn. Vi kommer att få en ännu bättre bild över vad vi egentligen utsätts för varje år.

Strategin har antagits. Fyra myndighetsuppdrag beslutades samma dag. Det är inte bara mål utan det är även fråga om pengar. Regeringen har lagt hela frågan om kontraktering och upphandling i ett särskilt spår. Där finns också oerhört mycket att göra.

Under många år tycks det ha varit något slags självändamål att outsourca, upphandla, privatisera och lägga så mycket som möjligt utanför staten. Anna Kinberg Batra stod i tv och sa att det inte spelar någon roll var servrarna står. Jo, det gör det visst i en del avseenden. Det som rör vår viktigaste information ska vi ha kontroll över. Lärdomen av vad som har hänt på Transportstyrelsen är att regelverket i dessa frågor måste skärpas.

Regeringen har en annan ingång. Vår ingång är inte att privatisera, outsourca eller lägga ut så mycket som möjligt. Vår ingång i diskussionen är alltid säkerheten först. Det är det som måste gälla vid hanteringen av den typen av information.

Därför gör vi två saker. Den ena är att vi har bett en särskild utredare, Stefan Strömberg, att se över frågan om var gränserna går för att göra den här typen av upphandlingar. Han fick det uppdraget i våras.

Den andra är att vi nu under hösten går fram med ett skarpt förslag om samrådsplikt och vetorätt för Säpo och Försvarsmakten i de här situationerna. När någon myndighet står i begrepp att outsourca eller lägga ut viss sådan här informationsteknik på andra leverantörer och i privata händer och det rör den här typen av säkerhetskänslig information ska man vara skyldig att samråda med Säkerhetspolisen och Försvarsmakten. Om Försvarsmakten och Säkerhetspolisen säger ”nej, det här kan ni inte göra eftersom det riskerar rikets säkerhet”, då ska myndigheten också lyda. Förslaget är alltså att det ska finnas vetorätt för de myndigheterna i de situationerna. Det är ett skarpt förslag och en förordningsändring som vi går fram med nu under hösten.

Anf. 6 PÅL JONSON (M):

Herr talman! Tack, justitieministern, för debatten! Jag har två korta kommentarer.

Resursförstärkningarna som tillförs Must, MSB och FRA gör vi i rätt bred politisk samsyn, vill jag tillägga. Det är en del av försvarsöverenskommelsen. Det är alltså inte bara regeringen som ska hyllas här, tycker jag, utan det är också vi inom oppositionen som har drivit på eftersom det här behöver förstärkas.

Det andra ministern säger är ”säkerheten först”. Det är ingen som delar den uppfattningen i dag, i det här säkerhetspolitiska läget. Problemet med Transportstyrelsen var ju att man bröt mot lagen och att det saknades sanktionsmöjligheter. Det var det som var själva cloun i problemet.

Avslutningsvis, herr talman, vill jag ta upp en tredje aspekt som är principiellt viktig i cybersäkerhetsstrategin men som faktiskt inte nämns. Det är frågan om Sverige ska ha en aktiv eller offensiv förmåga inom cy-

bermiljön. Ministern vet att det framgår i Försvarsberedningen och i inriktningspropositionen att vi ska ha förmåga till någon form av vedergällning om vi blir utsatta för ett storskaligt it-angrepp. Detta nämns inte i cybersäkerhetsstrategin. Det tycker jag är anmärkningsvärt.

Om den här funktionen, den aktiva eller offensiva cyberförmågan, ska vara effektiv måste den kommuniceras. Det är ju en förmåga som vi inte vill använda, men vi vill att vår omvärld ska veta om den. Om den ska fungera måste det kommuniceras var, när och hur den ska användas.

Jag undrar därför om ministern har en uppfattning om Sverige ska ha en aktiv cyberförmåga samt hur, var och när den i så fall ska användas. Finns det några tankar om doktrin- eller policyutveckling på det området?

Anf. 7 Justitie- och inrikesminister MORGAN JOHANSSON (S):

Herr talman! Den senare frågan får vi nog återkomma till i en särskild diskussion, för den är ganska bred.

För att ta upp tråden om eventuella sanktioner och vad man kan göra mot dem som gör fel skulle jag vilja erinra om att en av sakerna som inträffade efter händelserna på Transportstyrelsen var att det visade sig att det finns skarpa instrument för tillsynsmyndigheten att gå vidare med när man behöver göra det. När man uppdagade detta inledde Säkerhetspolisen en förundersökning som slutade i ett strafföreläggande och med att den dåvarande generaldirektören för Transportstyrelsen fick avgå.

Det är alltid bättre att förebygga saker än att behöva komma efteråt och utreda om det skulle leda till brott. Det är därför vi nu lägger fram förslaget om samrådsplikt och vetorätt för Försvarsmakten och Säpo i alla dessa situationer. Det innebär att man inte kommer att kunna gå vidare med någonting i det här avseendet om de risker finns som Säpo och Försvarsmakten pekade på i fallet med Transportstyrelsen.

Det är helt riktigt som Pål Jonson säger att det här är ett gemensamt ansvar, vilket också innebär gemensamma pengar. Jag har inga som helst problem med att säga att uppgörelserna som vi har gjort inom ramen för försvarspolitiken är oerhört bra på många områden – förstärkningen av det militära försvaret men också av det civila försvaret, för att se det i ett större sammanhang. Det är över 400 miljoner ytterligare till det civila försvaret per år som nu sätts av, och det är en rejäl slant för att kunna återupprätta också den delen av försvaret.

Den här frågan får vi säkert återkomma till. Ni ska veta att vi jobbar aktivt i regeringen för att även fortsättningsvis stärka cybersäkerheten.

Överläggningen var härmed avslutad.

§ 6 Anmälan om interpellationer

Följande interpellationer hade framställts:

den 21 september

2017/18:5 Operativ förmåga med tung kustrobot
av *Allan Widman* (L)
till försvarsminister Peter Hultqvist (S)

2017/18:6 Motorfrågan för Gripen E
av *Allan Widman* (L)
till försvarsminister Peter Hultqvist (S)

§ 7 Anmälan om frågor för skriftliga svar

Följande frågor för skriftliga svar hade framställts:

den 21 september

2017/18:24 Polygama äktenskap
av *Ann-Charlotte Hammar Johnsson* (M)
till statsrådet Åsa Regnér (S)
2017/18:25 Sparandet i Sverige
av *Helena Bouveng* (M)
till finansminister Magdalena Andersson (S)
2017/18:26 Traineejobb i välfärden
av *Jesper Skalberg Karlsson* (M)
till arbetsmarknads- och etableringsminister Ylva Johansson (S)
2017/18:27 Gripanden i Katalonien
av *Birgitta Ohlsson* (L)
till utrikesminister Margot Wallström (S)
2017/18:28 Systembolagets verksamhetsfrämmande opinionsbildning
av *Tina Acketoft* (L)
till närings- och innovationsminister Mikael Damberg (S)

§ 8 Anmälan om skriftliga svar på frågor

Skriftliga svar på följande frågor hade kommit in:

den 21 september

2017/18:3 Ett nationellt skogsprogram
av *Kristina Yngwe* (C)
till statsrådet Sven-Erik Bucht (S)
2017/18:5 Polisens prioriteringar och barnkonventionen
av *Christina Örnebjär* (L)
till statsrådet Åsa Regnér (S)
2017/18:6 En bra uppkoppling i hela Sverige
av *Anna Wallén* (S)
till statsrådet Peter Eriksson (MP)
2016/17:1904 Regeringens agerande rörande Findus i Bjuv
av *Ann-Charlotte Hammar Johnsson* (M)
till närings- och innovationsminister Mikael Damberg (S)

§ 9 Kammaren åtskildes kl. 9.24.

Sammanträdet leddes av förste vice talmannen.

Vid protokollet

ANN LARSSON

/Olof Pilo

Innehållsförteckning

Tryck: Elanders, Vällingby 2017