Naalakkersuisut fremsætter hermed følgende beslutningsforslag i henhold til § 33 i forretningsordenen for Inatsisartut:

Forslag til Inatsisartutbeslutning om, at Grønlands Selvstyre tilslutter sig, at lov om Center for Cybersikkerhed sættes i kraft for Grønland ved kongelig anordning.
(Naalakkersuisoq for Uddannelse, Kultur og Kirke)

1. Anordningens indhold
1.1 Den overordnede baggrund for forslaget
Forsvarets Efterretningstjeneste vurderer, at en høj cybersikkerhedstrussel er et grundvilkår i et digitaliseret land. På den baggrund må Naalakkersuisut konstatere, at cyberangreb udgør en væsentlig risiko for Grønland.

Nunavut i Canada er i 2019 blevet ramt af et voldsomt cyberangreb. Det samme gælder Georgien. Om det er et cyberangreb med en kriminel hensigt eller et cyberangreb fra en statslig aktør er principielt set ligegyldigt. Virkningen er den samme. Den offentlige administration bliver lammet.

Det danske rederiselskab Mærsk A/S og Høreapparatkoncernen Demant er tidligere blevet ramt af cyberangreb. Ifølge pressen forlyder det, at omkostninger ved genopretningen af deres it-systemer skal regnes i milliarder af kroner.

Naalakkersuisuts administration blev i 2015 ramt af et cyberangreb. Det lammede store dele af administrationen i op til 14 dage. Efter angrebet blev backup-politikken af it-systemerne ændret for at sikre en hurtigere genopretning af skadede data. Den ændrede backup-politik har vist sin styrke, når vores it-systemer har været under angreb siden. Digitaliseringsstyrelsen kan nu isolere og gendanne skadede data, mens it-systemerne stadig benyttes af medarbejderne.

Med den øgede interesse for det arktiske område og Grønland er det Naalakkersuisuts vurdering, at risikoen for cyberangreb mod vores it-systemer er øget væsentligt. I Forsvarets Efterretningstjenestes rapport "Efterretningsmæssig Risikovurdering 2019" er Arktis for første gang kommet øverst på risikolisten. Risikovurderingen beskriver stormagtsrivaliseringen i Arktis. I forhold til enkelte stormagter gennemgås deres interesse for Grønland og deres hidtidige brug af påvirkningskampagner i andre lande. Forsvarets Efterretningstjeneste har dog ikke fundet, at nogen af stormagterne har forsøgt sig med påvirkningskampagner i Danmark endnu.

I det danske forsvarsforlig for perioden 2018 – 2023 er det blevet besluttet at styrke indsatsen på cyber- og informationssikkerhedsområdet ved at investere yderligere 1,4 mia. kr. i Danmarks cyber- og informationssikkerhed.

Center for Cybersikkerhed varetager rollen som Danmarks nationale it-sikkerhedsmyndighed og er en del af Forsvarets Efterretningstjeneste. Forsvaret er tvunget tilsluttet. Statsorganer og statslige myndigheder kan tilslutte sig netsikkerhedstjenesten.

Sættes Lov om Center for Cybersikkerhed i kraft for Grønland, kan Inatsisartut og Naalakkersuisuts myndigheder tilslutte sig centerets netsikkerhedstjeneste. Naalakkersuisut ønsker at tilmelde Naalakkersuisuts myndigheder til netsikkerhedstjenesten for hermed bedre at kunne beskytte vores it-systemer mod ondsindede angreb og sikre et højt informationssikkerhedsniveau.

Det er Naalakkersuisuts vurdering, at en tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste er den bedste beskyttelse for Grønland på nuværende tidspunkt. Risikoen for, at vores it-systemer lægges fuldkommen ned, som det er sket i Nunavut og Georgien, er måske ikke meget høj; men hvis det sker, vil effekten være stor og ramme det grønlandske samfund voldsomt, og omkostningerne for landskassen vil være ganske betydelige. Dette skal sammenholdes med, at Grønland kun har ganske få personer med relevante kompetencer inden for cyber- og informationssikkerhed. Naalakkersuisut anbefaler derfor, at Lov om Center for Cybersikkerhed sættes i kraft for Grønland ved en kongelig anordning.

For at sikre samarbejdet med Center for Cybersikkerhed vil Naalakkersuisut oprette en enhed for cyber- og informationssikkerhed, der skal arbejde for et højt informationssikkerhedsniveau i vores informations- og kommunikationsteknologiske infrastruktur og for at sikre en meget større opmærksomhed om cyber- og informationssikkerhed i den offentlige forvaltning. Enheden skal også have til opgave at styrke det grønlandske erhvervslivs viden og interesse for at beskytte sig mod ondsindet cyberangreb.

Naalakkersuisut ønsker med dette beslutningsforslag at styrke både opmærksomheden og indsatsen for et højt niveau af cyber- og informationssikkerheden i det grønlandske samfund.

Forslaget er en udmøntning af tema 2 om Sikkerhed og Privatliv i Digitaliseringsstrategien for 2018 – 2020. Heri bestemmes det, at der skal etableres et lovgrundlag for en styrket indsats til sikring af et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur og oprettelse af en cyber- og informationssikkerhedsenhed til at varetage opgaven.

1.2 Hovedlinjerne i lovforberedelsen

Naalakkersuisut har samarbejdet med Forsvarsministeriet og Center for Cybersikkerhed om udformningen af anordningsforslaget og de tekniske muligheder for, at Naalakkersuisuts myndigheder kan blive omfattet af Center for Cybersikkerheds netsikkerhedstjeneste.

En af udfordringerne var, at Naalakkersuisuts administration har mange fælles it-systemer. Herved adskiller vores it-arkitektur sig fra den danske statsadministration, hvor de enkelte myndigheder, som hovedregel har deres egne it-løsninger og systemer.

Vores valg af fælles it-arkitektur betyder, at stort set alle Naalakkersuisuts myndigheder vil blive omfattet af netsikkerhedstjenesten. Udfordringen ved fælles it-systemer er ikke af teknisk karakter, men i forhold til behandling af personoplysninger.

Hvis Center for Cybersikkerhed i forbindelse med deres analyser af datapakker eller stationære data finder skadelig programmering eller uventet datatrafik, er det deres standardprocedure at tilbagesende oplysninger om trafikdataene eller datapakkerne til den myndighed, der er dataansvarlig for meddelelsen eller datapakken.

I vores sammenhæng ville det betyde, at oplysningen om skadelig programmering eller uventet datatrafik vil blive sendt til den dataansvarlige myndighed. Da vi har mange fælles it-systemer, vil denne procedure i bedste fald være et forsinkende led for at kunne reagere hurtigt på en opstået risiko. I værste fald vil der være risiko for, at meddelelsen ikke videresendes til Digitaliseringsstyrelsen, der er systemansvarlig for alle fælles it-systemer på nær økonomiske it-systemer.

Digitaliseringsstyrelsen skal som den myndighed, der har ressortansvar for cyber- og informationssikkerhed, straks træffe de fornødne foranstaltninger til beskyttelse af vores it-systemer, når der modtages en sikkerhedsmeddelelse fra Center for Cybersikkerhed.

For at løse problemstillingen om behandling af personoplysninger i forbindelse med en sikkerhedshændelse vil Naalakkersuisut oprette en særlig cyber- og informationssikkerhedsenhed. Enheden skal gives tilladelse til at behandle alle typer personoplysninger, når disse behandles i forbindelse med en sikkerhedshændelse. Hensynet til, at der skal handles hurtigt på sikkerhedshændelser for at imødegå og begrænse skadevirkningen af en hændelse også i forhold til andre personers personoplysninger, overstiger hensynet til den konkrete person, hvis personoplysninger faktisk behandles. Enheden skal snarest oplyse den dataansvarlige myndighed om sikkerhedshændelsen også med henblik på, at hændelsen kan have en sådan karakter, at den skal indberettes til Datatilsynet med information om, hvad der er gjort for at begrænse skaden for den pågældende og andre.

2. Hovedpunkter i forslaget

a) Gældende ret

Der er ikke tidligere lovgivet på dette område. Forslaget indeholder elementer, der vedrører forhold, der normalt er reguleret i retsplejeloven for Grønland og i persondataanordningen. Disse forhold er beskrevet nedenfor.

Center for Cybersikkerheds Netsikkerhedstjeneste

Naalakkersuisut finder, at det er nødvendigt at få regler herom. Regler, der balancerer behovet for kontrol, men også tilgodeser beskyttelsen af borgernes personlige oplysninger. Firewalls og antivirusprogrammer kan ikke alene beskytte vores it-systemer med borgernes personoplysninger. Antivirusprogrammer skal først lære en ny virus at kende, før den kan indgå i virusbekæmpelsen. Hacking af vores it-systemer beskytter de ikke imod, da dette ofte sker på grund af mangelfuld it-sikkerhed både teknisk og organisatorisk. Teknisk på grund af forældede it-systemer og hardware og organisatorisk på grund af menneskelige fejl.
Hacking kan både have til hensigt at ødelægge, men formålet kan også være at tappe os for oplysninger, hvilket er, hvad en statslig aktør oftest har til hensigt.

Ved at blive en del af CFCS netsikkerhedstjeneste vil der blive etableret et normalt billede af variationen af vores internetkommunikation. Herved kan det opdages, om der er forsøg på at hente eller sende oplysninger ud af vores it-systemer. Skulle vi blive udsat som den første for et virusangreb, bliver vi en del af et system, som søger hurtigst muligt at begrænse skaderne også for andre.

Indgreb i meddelelseshemmeligheden

Trafikdata indeholder data, som behandles elektronisk som et led i overførslen af internetbaseret kommunikation. Det er oplysninger, som er nødvendige for at en meddelelse kan komme frem til modtageren. Det er for eksempel email-adresser, hjemmesideadresser og ip-adresser.

Pakkedata indeholder selve den indholdsmæssige kommunikation, indholdet af en email eller den information, som tilgås på en hjemmeside.

CFCS indsamler trafikdata og pakkedata for at analysere dem for malware. CFCSs behandling har alene til formål at klarlægge sikkerhedshændelsernes karakter og er rettet mod tekniske oplysninger om sikkerhedshændelserne. For eksempel analyse af en virus i en fil.

Når Naalakkersuisut tilslutter sig CFCS sikkerhedstjeneste, giver Naalakkersuisut samtykke til, at trafikdata, pakkedata og stationære data må behandles. Det betyder, at borgere, der sender elektronisk post til Naalakkersuisuts administration, kan få deres meddelelse behandlet af CFCS, hvis meddelelsen indeholder malware. Det samme gælder for personalet i

Naalakkersuisuts administration, der benytter administrationens it-udstyr til at sende og modtage private meddelelser.

Naalakkersuisut finder, at afvejningen af hensynet til den enkelte skal vige for hensynet til helheden og samfundet. Det er væsentligt at beskytte alles personoplysninger mod skadelige sikkerhedshændelser.

Anordningsforslaget begrænser CFCSs adgang til at behandle personoplysninger. Formålet skal være at sikre et højt informationssikkerhedsniveau.

Påbud om udlevering af oplysninger på baggrund af kendelse (edition)
En sikkerhedshændelse kan være en strafbar handling eller et forsøg herpå. Efter politiets begæring kan retten efter retsplejeloven for Grønland § 184 som et led i efterforskningen af en strafbar overtrædelse pålægge en person, der ikke er mistænkt, at forevise eller udlevere information, der er undergivet vedkommendes rådighed.

I beslutningsforslaget gives CFCS ret til selv at opnå denne ret ved kendelse i Retten i Grønland. Bestemmelsen om edition kan anvendes til at få oplysninger om, hvem som på et givet tidspunkt var bruger af en specifik ip-adresse eller email-konto. CFCS samarbejder med politiet og udveksler oplysninger om efterforskning af sikkerhedshændelser, der gøres til en kriminalretslig undersøgelse.

Da CFCS også har til formål at imødegå og begrænse effekten af sikkerhedshændelser, har CFCS behov for at kunne få editionsoplysninger fra en tredjepart for at kunne vurdere karakteren og alvorligheden af en mistænkelig aktivitet. Herunder også at kunne underrette offeret for et cyberangreb om en kompromittering af vedkommendes it-systemer.

Forholdet til persondataanordningen
I persondataanordningens § 2, stk. 10 er det fastsat, at lovens bestemmelser for behandling af personoplysninger ikke gælder for politiets og forsvarets efterretningstjenester.

Beslutningsforslaget fastsætter, at de centrale principper i persondataanordningen så vidt muligt skal gælde for Center for Cybersikkerhed.

Retten til indsamling af personoplysninger skal ske til udtrykkeligt angivne og saglige formål og må ikke senere bruges til formål, der er uforenelige med disse formål.

Behandlingen af almindelige personoplysninger må ske efter tilsvarende kriterier som efter persondataanordningen.

Behandlingen af følsomme oplysninger, herunder helbredsoplysninger og seksuelle oplysninger må alene behandles efter samme betingelser som efter persondataanordningen. Tilsvarende gælder for særligt følsomme oplysninger, medmindre det er nødvendigt.

En fysisk eller en juridisk person har ikke aktindsigt i egne oplysninger indsamlet af CFCS, men kan klage til Tilsynet med Efterretningstjenesterne. Tilsynet har fået en særlig indsigtsret til at varetage denne form for klager. Tilsynet kan anmode CFCS om at undersøge, hvorvidt der uberettiget behandles oplysninger om den pågældende. Tilsynet sikrer i så fald, at det ikke er tilfældet. Tilsynet giver herefter den pågældende meddelelse herom.

b) Forslaget
§ 1 fastsætter, at Center for Cybersikkerhed (CFCS) har til opgave at sikre et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af. Den kommende Cyber- og Informationssikkerhedsenhed skal samarbejde med CFCS for at opnå denne målsætning i Grønland.

§ 2 definerer begreberne sikkerhedshændelse, pakkedata, trafikdata, stationære data, malware, personoplysning og behandling.

§ 3 fastsætter opgaverne for CFCSs netsikkerhedstjeneste. Opgaven er at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndighederne på Forsvarsministeriets område og hos tilsluttede myndigheder og virksomheder.

§§ 4 – 6 c omfatter indgreb i meddelelseshemmeligheden.

§ 4 fastsætter, at CFCS uden retskendelse kan behandle pakkedata, trafikdata og stationære data hidrørende fra netværk hos tilsluttede myndigheder med henblik på at sikre et højt informationssikkerhedsniveau i samfundet.

§ 5 fastsætter, at CFCS uden retskendelse kan behandle stationære data hidrørende fra netværk hos en myndighed eller virksomhed, der ikke er tilsluttet netsikkerhedstjenesten. Myndigheden eller virksomheden skal selv anmode CFCS om bistand. Behandling er betinget af, at behandlingen kan bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet.

§ 6 fastsætter, at CFCS efter aftale med en myndighed eller virksomhed ved en begrundet mistanke om en sikkerhedshændelse uden retskendelse kan blokere, omdanne eller omdirigere trafikdata og pakkedatadata. Ved en konstateret sikkerhedshændelse kan CFCS efter aftale med den tilsluttede myndighed eller virksomhed slette de stationære data, der har forårsaget sikkerhedshændelsen.

§ 6 a fastsætter, at CFCS ved rådgivning af en myndighed eller virksomhed om forebyggelse af sikkerhedshændelser kan gennemføre sikkerhedstekniske undersøgelser, når en myndighed eller virksomhed anmoder om det. Anmodningen kan give CFSC ret til uden retskendelse at behandle trafikdata, pakkedata og stationære data hos myndigheden eller virksomheden. Desuden ret til at behandle offentligt tilgængeligt materiale om myndigheden, virksomheden eller deres medarbejdere og til at iværksætte forebyggelsesaktiviteter rettet mod udvalgte medarbejdere eller enheder i myndigheden eller virksomheden.

§ 6 b fastsætter, at CFCS kan opsætte fiktive angrebsmål for at opnå viden om angrebsaktørers metoder og værktøjer, hvis det kan bidrage til et højt niveau af informationssikkerhed i samfundet.

§ 6 c fastsætter, at CFCS for at forhindre, standse eller begrænse en nært forestående eller igangværende sikkerhedshændelse kan gøre brug af domænenavne og tilsvarende it-infrastruktur, som anvendes eller har været anvendt af en angrebsaktør, forudsat at de er ledige.

§§ 7 til 7 d omfatter edition.

§ 7 fastsætter, at der til afdækning sikkerhedshændelser kan pålægges en juridisk eller fysisk person pligt til at udleve oplysninger om brugeren af en emailkonto, ip-adresse eller domænenavn.

§ 7 a fastsætter, at Retten i Grønland træffer afgørelse om pålæg efter § 7 efter CFCSs begæring. Retsmødet holdes for lukkede døre.

§ 7 b fastsætter, at inden Retten i Grønland træffer sin afgørelse, skal den, som har rådighed over oplysninger, have adgang til at udtale sig. Retten eller CFCS kan pålægge den, der har rådighed over oplysningerne, tavshedspligt.

§ 7 c fastsætter, at kære til højere ret finder anvendelse.

§ 7 d fastsætter, at CFCS har ansvaret for, at rettens kendelse udføres.

§ 8 fastsætter, at CFCS er undtaget fra den danske lov om offentlighed i forvaltningen undtagen notatpligten, endvidere væsentlige dele af den danske forvaltningslov (Kap. 4-6) samt den danske databeskyttelseslov herunder databeskyttelsesforordningen.

§ 8 a fastsætter, at oplysninger omfattet af denne lov skal overføres til arkiv efter reglerne i den danske arkivlov.

§ 8 b fastsætter, at myndigheders og virksomheders samarbejde med CFCS ikke er begrænset af bestemmelser om tavshedspligt fastsat ved lov eller med hjemmel i lov. Forsvarsministeren kan fastsætte nærmere regler herom.

§§ 9 til 14 svarer i sit væsentligste indhold til persondataanordningens behandlingsregler i §§ 5 til 8 for personoplysninger.

§ 15 fastsætter, at CFCS kan foretage automatiserede analyser af trafikdata, pakkedata, stationære data eller malware, der er indsamlet efter §§ 4 – 6 c. Manuelle analyser af data kan kun ske i nærmere afgrænsede tilfælde.

§ 16 fastsætter, at CFCS kan videregives trafikdata, pakkedata og stationære data til
1) Politiet
2) Den tilsluttede myndighed, virksomhed eller borger, hvorfra dataene stammer.
3) Til offentlige myndigheder, udbydere af offentlige elektroniske kommunikationsnet og –tjenester, andre netsikkerhedstjenester og virksomheder i forbindelse med udsendelse af sikkerhedsvarslinger ved begrundet mistanke om en sikkerhedshændelse.

Der knytter sig forskellige betingelser til videregivelsen, afhængig af om det videregivne er trafikdata, pakkedata, stationære data eller malware.

§ 17 fastsætter, at data skal slettes, når formålet med behandlingen er opfyldt. Dog kan CFCS opbevare data i højest
a) 5 år, når dataene knytter sig til en sikkerhedshændelse,
b) 3 år, når data ikke knytter sig til en sikkerhedshændelse, men som stammer fra myndigheder, som i særlig grad behandler udenrigs-, sikkerheds- og forsvarspolitiske forhold eller
c) 13 måneder for data, der ikke knytter sig til en sikkerhedshændelse.
d) Data videregivet i medfør at § 16 slettes ikke.

§ 17 a fastsætter, at data, der er deponeret på fiktive angrebsmål efter § 6 b eller modtaget via infrastruktur omfattet af 6 c, skal slettes hurtigst muligt. Hvis CFCS har udtaget dataene til nærmere analyse, sker sletning efter § 17.

§ 18 fastsætter, at CFCS skal træffe passende tekniske og organisatoriske foranstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, og mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Bestemmelsen svarer til persondataanordningens § 41, stk. 3.

§ 19 – 24 fastsætter Tilsynet med Efterretningstjenesternes pligter og rettigheder i forhold til CFCS.

§ 24 sættes ikke i kraft for Grønland. § 24 pålægger Tilsynet med Efterretningstjenesterne at afgive en årlig redegørelse om sin virksomhed til forsvarsministeren, og at redegørelsen offentliggøres.

Da redegørelsen offentliggøres, har både Inatsisartut og Naalakkersuisut adgang til at foretage kontrol af CFCS's aktiviteter, herunder at klage til Tilsynet med Efterretningstjenesterne efter § 20 eller benytte de andre muligheder, som rigsfællesskabet tilsikrer.

3. Økonomiske og administrative konsekvenser for det offentlige
Når en høj cybersikkerhedstrussel er et grundvilkår i den offentlige administration, er det nødvendigt, at offentlige myndigheder tager cybersikkerhedstruslen alvorlig. Der skal bruges både økonomiske og personalemæssige ressourcer på opgaven.

For at effektivisere opgaven ønsker Naalakkersuisut at etablere en central cyber- og informationssikkerhedsenhed. Enheden skal have kompetence til at fastsætte politikker og standarder for cyber- og informationssikkerheden samt at føre tilsyn med, at de overholdes i Naalakkersuisuts administration. Desuden skal enheden have kompetence til at behandle personoplysninger i forbindelse med sikkerhedshændelser.

En vigtig opgave for enheden er information og vejledning til borgere og virksomheder om cyber- og informationssikkerhed. At borgerne og virksomheder er og fortsat udvikler deres kompetenceniveau for at beskytte sig mod cyberangreb er vigtigt nu og i fremtiden endnu vigtigere. Det afgørende for det grønlandske samfund er, at der kommer til at være en stor modstandskraft mod, at samfundet bliver ramt af et ødelæggende cyberangreb.

Alle opgaverne skal enheden løse i samarbejde med Center for Cybersikkerhed.

Den årlige driftsomkostning af enheden vil være 5 mio. kr.

4. Økonomiske og administrative konsekvenser for erhvervslivet
Erhvervslivet skal fremover have øget fokus på cybersikkerhed og risikoen for et ødelæggende cyberangreb.

Med forslaget forventes det, at erhvervslivets omkostninger til cybersikkerhed kan reduceres og bruges mere effektivt, da Cyber- og informationsenheden vil være mellemled mellem virksomhederne og den viden som Center for Cybersikkerhed skaber om cybersikkerhed.

Cyber- og informationsenheden skal understøtte denne udvikling.

5. Konsekvenser for miljø, natur og folkesundhed
Der vil ikke være nogen konsekvenser for miljø, natur og folkesundhed.

6. Konsekvenser for borgerne
Borgerne skal ligesom erhvervslivet have øget fokus på farerne ved det åbne internet. Både med hensyn til beskyttelse af egne oplysninger på deres eget it-udstyr og på de farer, som de kan påføre andre i deres kommunikation med dem.

Cyber- og informationssikkerhedsenheden skal medvirke til, at borgerne får en øget viden om, hvordan den enkelte bedre kan beskytte sig.

7. Andre væsentlige konsekvenser
Der er ingen andre væsentlige konsekvenser.

8. Høring af myndigheder og organisationer
Forslaget har i perioden 15. januar 2020 til og med 12. februar 2020 været i offentlig høring på høringsportalen samt direkte fremsendt til følgende høringsparter:

Avannaata Kommunia	
Kommune Kujalleq	
Kommune Qeqertalik	
Kommuneqarfik Sermersooq	
Qeqqata Kommunia	
Naalakkersuisut Siulittaasuata Naalakkersuisoqarfia	Formandens Departement
Pinngortitamut Avatangiisinullu Naalakkersuisoqarfik	Departementet for Miljø og Natur
Aningaasaqarnermut Naalakkersuisoqarfik	Departementet for Finanser
Aatsitassanut Naalakkersuisoqarfik	Departement for Råstoffer
Ineqarnermut Attaveqaqatigiinnermullu Naalakkersuisoqarfik	Departementet for Boliger og Infrastruktur
Ilinniartitaanermut, Kultureqarnermut Ilageeqarnermullu Naalakkersuisoqarfik	Departementet for Uddannelse, Kirke, Kultur og Ligestilling
Nunanut Allanut Naalakkersuisoqarfik	Departementet for Udenrigsanliggender

Aalisarnermut Piniarnermut Nunalerinermullu Naalakkersuisoqarfik	Departementet for Fiskeri, Fangst og Landbrug
Peqqissutsimut Naalakkersuisoqarfik	Departementet for Sundhed
Isumaginninnermut, Inatsisinillu Atuutsitsinermut Naalakkersuisoqarfik	Departementet for Sociale Anliggende og Justitsområdet
Inuussutissarsiornermut, Nukissiuuteqarnermut Ilisimatusarnermullu Naalakkersuisoqarfik	Departementet for Erhverv, Energi, Forskning og Arbejdsmarked
Nunatsinni Nakorsaaneqarfik	Landslægeembedet
Bispekontoret	
Grønlands Politi	
Inuit Pisinnaatitaaffiinut Kalaallit Nunaata Siunnersuisoqatigiivi pillugit	Grønlands Råd for Menneskerettigheder
Kalaallit Nunaanni Naligiissitaanissamut Siunnersuisoqatigiit	Ligestillingsrådet i Grønland
MIO – Meeqqat Inuusuttullu Oqaloqatigiinnittarfiat	MIO – Børnerettighedsinstitutionen
Datatilsynet	
Institut for Menneskerettigheder	
Tilioq Nukissiorfiit Mittarfeqarfiit	Handicaptalsmand
Sulisitsisut Sulinermik Inuussutissarsiuteqartut Kattuffiat SIK	Grønlands Erhverv
Nunatsinni Advokatit	Grønlandske Advokater
Peqqissaasut Kattufiat	Grønlands Sygeplejerskeorganisation
Atorfillit Kattuffiat, AK	AK
Ilinniartitsisut Meeqqat Atuarfianneersut Kattuffiat, IMAK.	IMAK
NUSUKA	
Ilinniagartuut ASG	Akademikernes Sammenslutning i Grønland ASG

Tele-Post
GrønlandsBANKEN
Banknordic
Royal Artic Line
Air greenland
Kalaallit Airports

9. Høringssvar
Der er modtaget 9 høringssvar.
Generelt er der tilslutning til forslaget i en erkendelse af, at cyber- og informationssikkerhed er vigtig for Grønland. Høringssvarene har ikke givet anledning til ændringer i anordningsforslaget.

Tilslutning til netsikkerhedstjenesten
Flere høringssvar savner en mere uddybende beskrivelse af, hvilke opgaver som Center for Cybersikkerhed udbyder, som grundlag for at kunne træffe en beslutning om tilslutning til netsikkerhedstjenesten. Forslaget er et tilbud til myndigheder og virksomheder om at blive tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste, ikke en pligt.

Det fremgår af § 1 i den danske bekendtgørelse nr. 896 af 21. august 2019 om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste, at en tilslutningsaftale kan omfatte 1) opsætning og drift af en eller flere alarmenheder, 2) installation og drift af sikkerhedssoftware på lokale enheder, og 3) løbende overførsel af logoplysninger om konstaterede og mulige sikkerhedshændelser på eget sikkerhedssystem, herunder ved opsætning og drift af udstyr fra Center for Cybersikkerhed til håndtering af den løbende dataoverførsel. Desuden skal det af tilslutningsaftalen fremgå, om data hidrørende fra den tilsluttede myndighed eller virksomhed er omfattet af slettereglerne i enten § 17, stk. 2, nr. 2 eller 3 i lov om Center for Cybersikkerhed.

Det forventes, at et indhold svarende til § 1 vil være indeholdt i en kommende bekendtgørelse gældende for Grønland.

Når en myndighed eller virksomhed ønsker, at gå i dialog med Center for Cybersikkerhed om tilslutning udgør forslagets bestemmelser rammen for, hvorfor og hvordan Center for Cybersikkerhed må tilbyde ydelser, herunder at Center for Cybersikkerhed har ret til at afvise en tilslutning.

Hvordan en eventuel tilslutning teknisk skal ske, og hvilke hensyn, der skal varetages i forskellige henseender, er forskellig fra, om det er en kommune eller Tele-Post, der ønsker tilslutning. Finder myndigheden eller virksomheden ikke, at den opnåede tilslutningsaftale er tilfredsstillende, er de frie til at undlade at indgå en aftale. I henhold til forslaget er

bestemmelsen om Center for Cybersikkerheds ret til at give påbud om tilslutning ikke medtaget.

Cyber- og informationssikkerhedsenheden
Flere høringssvar kommenterer cyber- og informationssikkerhedsenheden og hvilken rolle den skal have.

Ved Naalakkersuisuts administrations tilslutning til netsikkerhedstjenesten skal der udpeges en myndighed, der skal være kontaktpunkt til Center for Cybersikkerhed.

Netsikkerhedstjenesten vil normalt, hvis der findes skadeligt software eller persondata med skadeligt software tilknyttet meddele det til den myndighed, de har indsamlet dataene fra. Forventningen er herefter, at myndigheden reagerer på det modtagne. Derudover skal der ske anmeldelse til Datatilsynet, hvis der er sket et databrud, og der skal tages de fornødne tekniske skridt til standsning, hindring eller inddæmning af en eventuel skadevirkning i it-systemerne. Da det kun er Digitaliseringsstyrelsen, der har adgang til den centralt opbyggede it-infrastruktur i Naalakkersuisuts administration, vil en sådan proces medføre en forsinkelse i processen med at begrænse skaderne, i værste fald en katastrofal forsinkelse.

For at sikre den hurtigst mulige reaktionstid for at begrænse eventuelle skadesvirkninger af et ondsindet angreb, skal en meddelelse fra netsikkerhedstjenesten gå direkte til nogen, som er forpligtet til at sikre en standsning, hindring eller inddæmning af skadesvirkningen.

Digitaliseringsstyrelsen har som en teknisk forvaltning ingen selvstændig kompetence til at behandle personoplysninger på andre myndigheders vegne. For at der kan ske en hurtig indsats imod et ondsindet angreb, der medfører behandling af personoplysninger i forbindelse med en sikkerhedshændelse, skal en enhed have denne bemyndigelse. Det betyder, at cyber- og informationssikkerhedsenheden skal være dataansvarlig for behandling af disse personoplysninger i forbindelse med en sikkerhedshændelse.

Cyber- og informationssikkerhedsenheden skal være ansvarlig for at sikre, at der straks gøres en indsats for standsning, hindring eller inddæmning af et ondsindet angreb. Enheden skal også straks meddele den oprindeligt dataansvarlige myndighed, at der er sket en sikkerhedshændelse. Er der sket et databrud, der skal anmeldes til Datatilsynet, skal enheden hjælpe den dataansvarlige myndighed med indberette databruddet og bistår med vurderingen af skadens omfang for de berørte privatpersoner til Datatilsynet.

Cyber- og informationsenheden har som en offentlig myndighed vejledningspligt til borgere og virksomheder om cybersikkerhed. Forslaget pålægger enheden en skærpet vejledningspligt, som beskrevet tidligere i bemærkningerne.

Behandling af personoplysninger
Datatilsynet har i sit høringssvar pointeret, at enhver behandling af personoplysninger udført af grønlandske myndigheder skal ske i overensstemmelse med persondataanordningen, herunder videregivelse af personoplysninger til Center for Cybersikkerhed, som følge af dette forslag.

Datatilsynet henviser ligeledes til, at det er klart, hvem der er dataansvarlig i forbindelse med en behandling af personoplysninger, herunder navnlig i det omfang der som følge af forslaget sker videregivelse mellem flere grønlandske myndigheder.

Til orientering har Datatilsynet vedlagt et tidligere afgivet høringssvar til Forsvarsministeriet ved den seneste ændring af Lov om Center for Cybersikkerhed.

Heri påpeger Datatilsynet, at selv om databeskyttelsesforordningen og databeskyttelsesloven ikke gælder for Center for Cybersikkerhed, gælder de for alle de tilsluttede myndigheder og private virksomheder. Det betyder for Grønland, at persondataanordningen gælder for de tilsluttede myndigheder og private virksomheder.

Desuden påpeger Datatilsynet, at en sikkerhedshændelse efter forslaget må anes som et brud på persondatasikkerheden, der skal anmeldes til Datatilsynet.

Høringssvaret til Forsvarsministeriet er afgivet i forhold til den danske databeskyttelseslov og databeskyttelsesforordningen. De bestemmelser, der henvises til i høringssvaret til databeskyttelsesforordningen, har tilsvarende bestemmelser i persondataanordningen.
De tanker og vurderinger, der indgår i høringssvaret, vil indgå i det videre arbejde med at fastsætte opgaver og ansvar for cyber- og informationsenheden og dets samarbejde med henholdsvis Center for Cybersikkerhed og Naalakkersuisuts myndigheder.

Nr.	**Høringspart**	**Bemærkning**	**Kommentar til bemærkning**
1	Kommune Kujalleq	Efter anordningsforslagets § 3, stk. 3, kan ”kommuner og virksomheder, der har samfundsvigtig karakter, efter anmodning blive tilsluttet netsikkerhedstjenesten, såfremt Center for Cybersikkerhed konkret vurderer, at tilslutningen vil kunne bidrage til at understøtte et højt	Anordningsforslagets § 3, stk. 3 har to kriterier for at en kommune eller virksomhed kan blive tilsluttet netsikkerhedstjenesten. Kommunen eller virksomheden skal have samfundsvigtig karakter og tilslutningen vil kunne bidrage til at understøtte et højt

		informationssikkerhedsniveau i samfundet." Kommune Kujalleq mener, at det i såvel resuméet af anordningsforslaget som i beslutningsforslaget til Inatsisartut bør beskrives lidt mere udførligt, hvilke opgaver som netsikkerhedstjenesten udbyder, så kommunerne får et bedre grundlag for at overveje, om det er relevant at søge tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste, og hvilke sagsbehandlingsregler som gælder. Ovenstående begrundes med henvisninger til de almindelige bemærkninger til forslaget til lov nr. 555 af 7. maj 2019 om ændringer af lov om Center for Cybersikkerhed. De citerede dele af bemærkningerne er henset til omfanget ikke medtaget.	informationssikkerhedsniveau i samfundet. Begge kriterier vil indgå i bedømmelsen af, om en kommune eller en virksomhed vil kunne omfattes af Center for Cybersikkerheds ydelser. Ingen af kriterierne er stationære. Samfundsudviklingen kan ændre sig og flytte forståelsen af, hvad der bliver anset for være omfattet af kriteriet samfundsvigtig karakter. Ligeledes vil forståelse af et højt informationssikkerhedsni-veau ændre sig. Det som blev anset for sikkert for få år siden, anses i dag for usikkert. Den digitale udvikling vil hurtigt ændre forståelsen af kriteriet et højt informationssikkerhedsni-veau. For at kommunerne og virksomheder kan få gavn af forslaget er det dog ikke en forudsætning, at de faktisk er tilsluttet netsikkerhedstjenesten. Den foreslåede Cyber- og informationssikkerhedsenhed har til opgave at sikre, at den viden og erfaring, som

			udvikles i Center for Cybersikkerhed kommer til gavn i grønlandske kommuner og virksomheder. Den viden og erfaring, som Center for Cybersikkerhed indsamler, dannes på baggrund af de tilsluttede myndigheder og virksomheders konstaterede cyberangreb og dets deltagelse i et internationalt samarbejde. Den danske bekendtgørelse nr. 836 af 21. august 2019 om tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste er rammen for de tilsluttede myndigheder og virksomheders samarbejde med Center for Cybersikkerhed. En tilsvarende bekendtgørelse forventes ikraftsat for Grønland. Bekendtgørelsens § 1 er beskrevet i afsnit 9 Høringssvar i underafsnittet Tilslutning til netsikkerhedstjenesten.
2	Sulinermik Inuussutissarsiu-teqartut Kattuffiat SIK	SIK kan bakke op om intentionerne i forslaget, idet forslaget ses at ville forebygge Cyberangreb mod bl.a. den offentlige administration. SIK noterer samtidigt, at tilslutning til Cyber- og Informationssikkerhedsenheden	Støtte til forslaget

		vil medvirke til, at borgerne får en øget viden om, hvordan den enkelte bedre kan beskytte sig – og det er jo positivt. SIK støtter derfor forslaget til Inatsisartutbeslutning.	
3	Sulisitsisut Grønlands Erhverv	Grønlands Erhverv (GE) finder selve ideen om at tilslutte sig Center for Cybersikkerhed for nødvendig, således at Grønland beskyttes på bedst mulig måde imod ukendte og vira og hackerangreb.	Støtte til forslaget
		<u>Oprettelse af særlig cyber- og informationssikkerhedsenhed i Naalakkersuisut</u> Grønlands Erhverv støtter oprettelsen af en "særlig cyber- og informationssikkerhedsenhed", da behandlingen af følsomme persondata og andre oplysninger kræver viden og fokus. Men i det omfang, at denne enhed skal agere over for de mulige trusler, som Grønland i IT henseende måtte blive udsat for, vil det vigtigste for erhvervslivet og for borgerne være at blive gjort klart, hvilken trussel der søges dæmmet op for. Heri ligger formentlig det problem, at truslerne er så mangeartede. Dette vil kunne svække forståelsen for den indsats, der søges dæmmet op for, når/hvis indsatsen imod sådanne trusler risikerer at	Cyber- og informationssikkerhedsenhedens hovedformål er at skabe opmærksomhed om cyber- og informationssikkerhed. Den største risiko i forbindelse med et ondsindet angreb er den menneskelige faktor. En person modtager en "spændende" email fra en ukendt afsender. Den skal åbnes. Ved åbningen aktives et skjult program, der kommer til at give adgang til de bagved liggende it-systemer eller noget så simpelt som at password er for lette at gætte. Når en ondsindet angriber har et brugbart password er der fri adgang til it-systemer uden om firewalls og tekniske hindringer. Truslerne er mangeartede og forandrer sig over tid. Det er

		hæmme de offentlige it-systemer, som der redegøres for i bemærkningerne til forslaget. Omvendt finder GE det positivt, at samme enhed får til "opgave at styrke det grønlandske erhvervslivs viden og interesse for at beskytte sig mod ondsindet cyberangreb". Da de faglige forudsætninger for at bestride det ansvar og udføre de opgaver, der er forbundet med formålet hermed, forudsættes at skulle være af høj kvalitet, efterlyses et svar på, hvorfra disse kvalificerede medarbejdere skal skaffes. GE ønsker på ingen måde at decimere de it-mæssige forudsætninger, det p.t. findes her i landet. Men såfremt der fra dansk side investeres 1,4 mia. kr. for at håndtere Danmarks cyber- og informationssikkerhed, kunne man godt forvente, at de p.t. tilstedeværende faglige forudsætninger i Grønland næppe vil være tilstrækkelige. Med de problemer, man på andre områder har med at skaffe specialviden, forekommer dette som en latent trussel i Grønland imod formålet i det stillede forslag.	heller ikke cyber- og informationssikkerhedsenhe-dens opgave at forebygge cyberangreb. Er angrebet sket, er det it-driftsafdelingens suveræne opgave at medvirke til at genoprette normal it-drift igen. Cyber- og informationssikkerhedsenhede n skal være med til at opbygge procedurer og processer, der skal søge at forhindre eller begrænse skadevirkningen af et ondsindet angreb. Den viden herom, som enheden opnår, skal den dele med alle, der har behov herfor. Det er borgere, således at de bedre kan beskytte sig. Det er virksomheder store som små, - et ondsindet angreb kan have en voldsom effekt på virksomhederne, og i værste fald kan virksomhedens eksistens være truet. De faglige forudsætninger er en udfordring. De skal opbygges. Til det fremtidige samarbejde påregnes der udarbejdet en samarbejdsaftale med Center for Cybersikkerhed. Heri vil indgå uddannelse og efter- og videreuddannelse af cyber- og informationssikkerhedsenhede ns medarbejdere. Ambitionen er, at enheden skal præstere på

			et højt kvalitetsniveau. Det høje kvalitetsniveau skal ske i et samarbejde med Center for Cybersikkerhed. De 1,4 mia. kr. fra dansk side er en merbevilling til cyber- og informationssikkerhedsområdet i det nuværende forsvarsforlig. Driftsbevillingen fra det forrige forsvarsforlig er fortsat i det nye forsvarsforlig. De 1,4 mia. kr. er alene et udtryk for, at Danmark har anset det for nødvendigt at styrke området for, at det fortsat kan sikre højt informationssikkerhedsniveau i den informations- og kommunikationsteknologoske infrastruktur, som samfundsvigtige funktioner er afhængige af.
		<u>Center for Cybersikkerheds rolle og arbejde i Grønland (CFCS)</u> Hvorledes kontrolleres og hvordan forstås CFCS´ adgang til – specielt – pakkedata? Det oplyses, at CFCS´ behandling heraf ”alene har til formål at klarlægge sikkerhedshændelsernes karakter og er rettet mod tekniske oplysninger om sikkerhedshændelser” Ikke desto mindre gives CFCS adgang til den indholdsmæssige	Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste. Sammen med Politiets Efterretningstjeneste kontrolleres de af Tilsynet med Efterretningstjenesterne. Tilsynet med Efterretningstjenesterne er reguleret i lov om Politiets Efterretningstjeneste. På Inatsisartuts forårssamling 2020 behandledes Forslag til Inatsisartutbeslutning om, at Grønlands Selvstyre tilslutter sig udkast til Anordning om

		kommunikation i f.eks. en e-mail korrespondance, og kontrol af, hvorledes dette håndteres, synes derfor nødvendig. Denne mulighed ligger – så vidt GE kan læse ud af bemærkningerne – uden for de tilfælde, hvortil der kræves dommerkendelse, hvor en person pålægges " at forevise eller udlevere information, der er undergivet vedkommendes rådighed"	ikrafttræden for Grønland af lov om Politiets Efterretningstjeneste. Forslaget blev vedtaget. Der henvises hertil for en nærmere forklaring om tilsynets udpegelse og funktion. Behandlingen af data sker ved en automatiseret proces, hvilket vil sige teknisk. Først når den automatiserede proces har fundet noget mistænkeligt, vil det blive behandlet af mennesker. Findes det skadelig software (malware) tilknyttet dataene, vil Center for Cybersikkerhed give besked til den tilsluttede, for at den tilsluttede kan handle på det fundne, nemlig at forhindre yderligere skader i it-systemerne. Er malware tilknyttet en personoplysning afsendt fra en borger, skal vedkommende også have besked herom i henhold til persondataanordningen.
		Til bestemmelserne i forslaget bemærkes, at forslaget inkorporerer bestemmelser fra databeskyttelsesforordningen. Man har til dato "kun" besluttet at i kraftsætte den "gamle" danske persondatalov i Grønland, hvorfor spørgsmålet går på, hvorledes dette harmonerer med indførelsen af de danske/EU-	Da Center for Cybersikkerhed er en del af forsvarsområdet, gælder hverken databeskyttelsesloven eller GDPR (databeskyttelsesforordningen) for Center for Cybersikkerhed. Derfor skal lov om Center for Cybersikkerhed indeholde

		retlige regler. Skal Grønland indføre GDPR lovgivning fra EU, og hvad er i givet fald tidsfaktoren herfor?	egne bestemmelser for behandling af personoplysninger. For tilsluttede myndigheder eller virksomheder i Grønland vil persondataanordningen gælde. Om Grønland skal anmode om en databeskyttelseslov for Grønland med GDPR er ikke et spørgsmål, der har betydning i denne sammenhæng.
		§ 17 fastsætter, at data skal slettes, når formålet med behandlingen er opfyldt. Når man samtidig har en bestemmelse i § 17 c), der tilkendegiver, at data, der ikke knytter sig til en sikkerhedshændelse, kan opbevares i 13 måneder, fanger denne vel sagtens al anden opbevaring af data. Hovedreglen i § 17 forekommer derfor hul.	13 måneders reglen var tidligere en 12 måneds-regel. Begrundelsen for at forlænge var, at det ikke var muligt at danne en årsvariation af data-flowet fra en tilsluttet myndighed eller virksomhed. Med et årsbillede af data-flowet er det blevet muligt at se, om variationerne er normale, eller de skyldes ondsindet downloading af data. At nogen eller noget henter data ud af it-systemerne. Hovedreglen er stadig relevant. Reglen er en generel regel i indeholdt i persondataanordningen. Ingen myndighed eller virksomhed må lave dataophobning. Data må kun opbevares, så længe det er relevant.
		Endelig mangler GE i forslaget til	Center for Cybersikkerhed

		Inatsisartutbeslutning information om, hvilke omkostninger der vil være forbundet med at tilslutte sig netsikkerhedstjenesten	afholder deres egne omkostninger, herunder omkostninger for det udstyr, der opsættes til indsamlingen af data. For den tilsluttede kommune eller virksomhed vil der være omkostninger til biydelser som husrum og energi samt de organisationsressourcer, der skal anvendes på samarbejdet med Center for Cybersikkerhed.
4	Tele-Post	TELE-POST ser generelt positivt på ikraftsættelsen af lov om Center for Cybersikkerhed, der vurderes at styrke informationssikkerhedsniveauet for Grønland, og vil, såfremt lovgivningen træder i kraft, indgå i samarbejde med CFCS i det omfang det skulle være ønsket.	Støtte til forslaget
		Det er TELE-POSTs opfattelse at netsikkerhedstjenesten, såfremt TELE-POST måtte blive tilmeldt denne, kun vil bruges til monitorering af TELE-POSTs administrative net, og at de grønlandske kunder ikke vil blive monitoreret med denne tjeneste. Det er dog uklart for TELE-POST hvor CFCS definerer grænsen mellem administrative data, og kundedata, og der opfordres i den forbindelse til dialog mellem de påvirkede myndigheder og virksomheder ved ikrafttrædelse af lovgivningen. TELE-POST kan ud fra det	Kommentaren er meget konkret om Tele-Post og om en eventuel tilslutning til netsikkerhedstjenesten. Det konkrete kræver en konkret stillingtagen. Hensigten med resumé og bemærkningerne er ikke at være et endeligt beslutningsgrundlag for, om en virksomhed tilslutter sig netsikkerhedstjenesten. Forslaget sætter rammerne for, hvad Center for Cybersikkerhed må eller ikke må. Den økonomiske afvejning af

		tilgængelige materiale ikke vurdere omfanget af ressourcer der skal allokeres til at administrere følgerne af denne lovgivning. Det angives i beslutningsoplæggets afsnit 4 at erhvervslivets omkostninger til cybersikkerhed kan reduceres som følge af denne lovgivning. Dette forventes ikke at være resultatet i TELE-POSTs tilfælde. Uagtet om lovgivningen træder i kraft, og der etableres en Cyber- og informationsenhed, har TELE-POST selv ansvaret for at sikre sikkerheden for selskabet og vores kunder, og vil egenhændigt iværksætte alle tiltag der vurderes relevante for at leve op til dette ansvar. Opgaver der kommer som følge af denne lovgivning vil komme i tillæg til den indsats TELE-POST allerede laver på sikkerhedsområdet.	hensynene til økonomi, ressourcer og risikoen for et ondsindet angreb og dets omkostninger er enhver virksomhedsledelses beslutning Bekendtgørelse nr. 836 af 21. august 2019 § 1 kan give yderligere anvisninger. § 1 er beskrevet i afsnit 9 Høringssvar i underafsnittet Netsikkerhedstjenesten.
		Af forslaget fremgår det at § 24 ikke kommer til at gælde for Grønland. Det anbefales at der enten etableres et tillæg til den beskrevne redegørelse der vedrører Grønland, eller der udarbejdes en separat redegørelse for Grønland, fremfor at de grønlandske aktiviteter blot indgår i redegørelsen gældende for Danmark, for at sikre transparens omkring de grønlandske aktiviteter.	Center for Cybersikkerheds årsrapport til forsvarsministeren bliver offentliggjort. Naalakkersuisut vurderer, at det vil give en tilstrækkelig transparens. Ligeledes formoder Naalakkersuisut, at sikkerhedsomstændigheder, der knytter sig til Grønland, kommer til at indgå i årsrapporten.
5	Nukissiorfiit	Som en virksomhed, der leverer kritisk infrastruktur, ser Nukissiorfiit særdeles positivt på,	Støtte til forslaget

		at Naalakkersuisut vil styrke cybersikkerhed i landet ved at blive omfattet af lov om Center for Cybersikkerhed gennem en kongelig anordning. Grønland er et af de mest digitaliserede lande i verden og er samtidig geografisk placeret mellem 2 søveje tæt ved Nordpolen, hvor der er stigende international opmærksomhed på det arktiske område. Dette kan medvirke til at forstærke risici for cyberangreb og i særdeleshed omkring infrastruktur. Nukissiorfiit hilser velkomment, at der gennem CFCS opnås større beskyttelse, samt at der bliver tilført viden på området, i erkendelse af egne og landets ressourcer til effektivt at kunne håndtere cyberangreb, som truer vores infrastruktur og datasikkerhed, ikke er tilstrækkelige.	
		Nukissiorfiit finder det betænkeligt: - at person- og databeskyttelse så omfattende bliver tilsidesat i anordningen i § 4, 5 og 6, hvor CFCS uden dommerkendelse kan indhente personoplysninger på udvalgte medarbejdere og tilgå kundeoplysninger, der ikke er offentlige samt at behandle data. Som det fremstilles bliver Nukissiorfiit hverken underrettet før eller efter et sådant tiltag. Der bør som minimum indføjes en underretningspligt, således at eventuelle berørte personer kan	Aktiviteter efter §§ 4-6 kan kun ske, hvis myndigheden eller virksomheden har tilsluttet sig netsikkerhedstjenesten. Ved tilslutningen tages der konkret stilling til § 4. Formålet med tilslutningen er at få behandlet trafikdata, pakkedata og stationære data. § 5 nr. 1 fordrer samtykke af den myndighed eller virksomhed, der skal undersøges. Om det er Center for Cybersikkerhed, der

		frikendes og virksomhederne får kendskab til, hvad CFCS har foretaget.	henvender sig til en myndighed eller virksomhed med en begrundet mistanke om en hændelse, eller det er en myndighed eller virksomhed, der er initiativtager, ændrer ikke ved, at det kun kan ske med myndighedens eller virksomhedens samtykke. § 5, nr. 2 er begrundet i samfundets interesse. Det er i samfundets interesse, hvis en myndighed eller virksomhed er kilde til gentagne ondsindede angreb, at dette stoppes. I § 6 er kravet også, at en myndighed eller virksomhed er tilsluttet netsikkerhedstjenesten. Derfor er dette også en af overvejelserne, som myndigheden eller virksomheden skal forholde sig til ved tilslutningen. Hvis data skal beskyttes, er det nødvendigt, at der kan handles hurtigt for at beskytte de øvrige data. Når en myndighed eller virksomhed tilsluttes, er det et krav fra Center for Cybersikkerheds side, at medarbejderne oplyses om, at der vil ske overvågning af datatrafikken.

			Når en myndighed eller virksomhed tilsluttes, skal der etableres et samarbejde med Center for Cybersikkerhed, i det mindste ved en udpegning af kontaktperson.
		- at CFDS får mulighed for at udgive sig som Nukissiorfiits medarbejdere og lokke andre medarbejdere til at begå ulovlighed. Nukissiorfiit finder det stærkt bekymrende, at sådanne aktiviteter påtænkes legaliseret.	En væsentlig del af et højt cyber- og informationssikker-hedsniveau er en myndigheds eller virksomheds medarbejdere. Cyberkriminelle søger at lokke password fra medarbejdere for at få adgang til it-systemerne. De passwords, som medarbejderne vælger, kan være for simple mm. Viser resultatet af en sådan undersøgelse, at medarbejdernes disciplin omkring password er for ringe, er det op til ledelsen at tage stilling til, hvordan dette kan forbedres.
		- at CFDS får mulighed for at installere software, som kan påvirke Nukissiorfiits systemer, og CFDS kan ikke garantere, at det ikke påvirker eller beskadiger Nukissiorfiits systemer. Dette kan have forsyningsmæssige konsekvenser, såvel som økonomiske konsekvenser.	Center for Cybersikkerhed får ikke mulighed for selv at installere noget software. En tilslutning er frivillig. I forbindelse med tilslutningen vil det være en væsentlig del af de tekniske undersøgelser for, hvordan overvågningen kan etableres, og ikke skader myndigheden eller virksomhedens funktioner eller opgaver.
		- at det ikke fremgår, af hvem og	De 5 mio. kr. er

		hvordan den årlige drift af enheden på 5 mio. skal finansieres. Det er Nukissiorfiits holdning, at det skal være Forsvaret, som afholder denne omkostning, da CFDS aktiviteter foretages ift. national sikkerhed.	Naalakkersuisuts omkostninger ved at tilslutte Naalakkersuisuts administration til netsikkerhedstjenesten. Omkostningerne skal finansieres ved en bevilling hertil på finansloven. Det skal i denne forbindelse bemærkes, at enheden er en del af Naalakkersuisuts administration, og at enheden varetager opgaver relateret til cyber- og informationssikkerhed i det grønlandske samfund. Dette kan, afhængig af sikkerhedshændelsens karakter og omfang også berøre rigets sikkerhed, men det kan også alene være en hændelse, som vedrører borgernes, myndigheders eller virksomheders sikkerhed i Grønland. Af disse midler skal også udføres oplysningsvirksomhed over borgere og virksomheder. Enhver tilslutning til netsikkerhedstjenesten vil indebære omkostninger for den tilsluttede. Center for Cybersikkerhed betaler for overvågningen og det udstyr, der bruges til overvågning.
		Slutteligt vil Nukissiorfiit gøre	Den generelle offentlige

		opmærksom på, at det *ikke* er god forvaltningskik med et så vigtigt og omfattende materiale, at 6 ugers høringsperioden *ikke* bliver respekteret og overholdt.	høringsperiode er 4 uger, og den er overholdt.
6	Datatilsynet	Datatilsynet forudsætter, at enhver behandling af personoplysninger udført af grønlandske myndigheder vil ske i overensstemmelse med persondataloven, herunder videregivelse af personoplysninger til Center for Cybersikkerhed som følge af anordningen. Datatilsynet henviser overordnet til, at det i denne forbindelse er en forudsætning, at det er klart, hvem der anses for dataansvarlig i forbindelse med en behandling af personoplysninger, herunder navnlig i det omfang der som følge af anordningen sker videregivelse mellem flere grønlandske myndigheder. Den dataansvarlige er efter persondatalovens § 3, nr. 4, den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger.	Oprettelse af Cyber- og informationssikkerhedsenheden er begrundet i at kunne leve op til persondataanordningens krav. Formålet er at gøre cyber- og informationssikkerhedsenheden dataansvarlig for behandling af personoplysninger i forbindelse med en sikkerhedshændelse. Grundet Naalakkersuisuts administrations centraliserede it-struktur er det nødvendigt med dette mellemled ud til Naalakkersuisuts myndigheder. Regelsættet omkring cyber- og informationssikkerhedsenhe-den skal sikre hjemmelsgrundlag for overførsler af personoplysningerne mellem myndighederne.
		Datatilsynet kan til orientering oplyse, at tilsynet i forbindelse	Datatilsynets bemærkninger til det danske lovforslag vil

		med en høring over udkast til forslag til lov om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden), Forsvarsministeriets sagsnummer 2018/006599, kom med bemærkninger vedrørende en række af de bestemmelser med databeskyttelsesmæssig relevans, der med nærværende forslag skal træde i kraft for Grønland. Datatilsynets tidligere bemærkninger, der relaterer til behandling af personoplysninger omfattet af databeskyttelsesforordningen og databeskyttelsesloven vedlægges dette brev til orientering. Disse bemærkninger er henset til deres omfang ikke citeret her.	indgå i udarbejdelsen af regelgrundlaget for cyber- og informationssikkerhedsenheden s funktion og status.
7	Departementet for Udenrigsanliggender	Det bemærkes, at forsvars- og sikkerhedspolitiske anliggender er et rigsanliggende, jf. selvstyrelovens § 11, stk. 3. Det bør derfor overvejes i hvilket omfang Naalakkersuisut ønskes inddraget/inddrages ved oprettelsen af en "lokal" Cyber- og informationssikkerhedsmyndighed".	Den foreslåede cyber- og informationssikkerhedsenhed er en enhed under Naalakkersuisuts administration. Enheden vil være underlagt en Naalakkersuisoq og indgå i Naalakkersuisuts ressortfordeling. Formålet med enheden er, at enheden skal være Naalakkersuisuts myndighedernes kontaktpunkt til Center for Cybersikkerhed vedrørende cyber- og

			informationssikkerhed. Som kontaktpunkt til Center for Cybersikkerheds er det enhedens opgave at sikre den interne kommunikation i Naalakkersuisuts administration. I afsnit 9 høringssvar er denne kommunikation nærmere beskrevet. Enhedens skal ikke beskæftige sig med forsvars- og sikkerhedspolitik. Det kan ikke afvises, at enheden vil komme til at beskæftige sig med problemstillinger afledt heraf.
		Danmarks nationale It-sikkerhedsmyndighed er underlagt et særligt uafhængigt kontrolorgan. Tilsynet består af fem medlemmer, der er udpeget af justitsministeren efter forhandling med forsvarsministeren. Formanden, der skal være landsdommer, er udpeget efter indstilling fra præsidenterne for Østre Landsret og Vestre Landsret, mens de øvrige medlemmer er udpeget efter drøftelse med Folketinges Udvalg vedrørende efterretningstjenesterne. Anordningen sætter ikke særlige tilsynsbestemmelser i kraft i Grønland, men forudsætter at tilsynet i Danmark varetager opgaven. Idet adgangen til nettet i	Det nævnte kontrolorgan er Tilsynet med Efterretningstjenesterne. Tilsynet er lovreguleret i lov om Politiets Efterretningstjeneste. Et Forslag til Inatsisartutbeslutning om, at Grønlands Selvstyre tilslutter sig udkast til Anordning om ikrafttræden for Grønland af lov om Politiets Efterretningstjeneste blev vedtaget på Inatsisartuts forårssamling 2020. Det er fremført i forhandlingerne med Forsvarsministeriet, at det er et ønske, at Naalakkersuisut kan udpege et medlem af tilsynet.

		Grønland er vidtgående, bør det overvejes at også Grønland udpeger et medlem til tilsynet eller deltager i processen om udpegning af medlemmer til tilsynet.	Forsvarsministeriet har ikke afvist ønsket, men det skal forhandles med Justitsministeriet. Imødekommes ønsket, skal det ske ved en ændring af lov om Politiets Efterretningstjeneste.
		Ikrafttræden af Lov om Center for Cybersikkerhed forudsætter ikke i sig selv oprettelse af en særskilt "cyber- og informationssikkerhedsenhed". Så forslaget om at oprette en sådan enhed må forstås som et ønske om udvidelse for at styrke og effektivisere indsatsen på cyber- og informationssikkerhedsområdet ift myndigheder, virksomheder og borger ud over de opgaver der i dag varetages af Digitaliseringsstyrelsen og Selvstyrets eksterne it-revision.	Ja, det er korrekt. Selve ikraftsættelsen af anordningen kræver ikke oprettelse af cyber- og informationsenheden, men Naalakkersuisuts tilslutning til Center for Cybersikkerheds netsikkerhedstjeneste gør. Enheden vil være nødvendig som kontaktpunkt for Center for Cybersikkerhed og til behandling af personoplysninger i forbindelse med en sikkerhedshændelse. Se mere udførligt i afsnit 9 Høringssvar
8	Departementet for Sundhed	Sundhedsvæsenets journalsystem er et meget decentralt system med, relativt set, et stort antal brugere, og dermed sårbart over for cyberangreb. Ikraftsættelse af den kgl. anordning må antages at kunne styrke IT-sikkerheden. Departementet for Sundhed kan tilslutte sig det fremlagte forslag	Støtter forslaget

		til etablering af Center for Cybersikkerhed, der skal understøtte og sikre et højt informations-sikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner i Grønland er afhængige af.	
9	Departementet for Finanser	Departementet for Finanser har ingen bemærkninger til beslutningsforslaget og anordningen i sin fremsendte form. Finansdepartementet sætter pris på tiltaget, og anerkender de store konsekvenser og omkostninger som et ondsindet netværks angreb kan betyde for både samfundet og virksomheder, men også borgere.	Støtter forslaget
10	Ilinniartitsisut Meeqqat Atuarfianneersut Kattuffiat, IMAK	Bestyrelsen for IMAK støtter beslutningsforslaget	Støtter forslaget