Bilaga 1: Handlingsplan

Nationell strategi för cybersäkerhet 2025–2029

Regeringskansliet
Försvarsdepartementet

Handlingsplan

Till strategins pelare och mål kopplas denna handlingsplan som innehåller ett antal aktiviteter som svarar mot regeringens inriktning och kraven i NIS 2-direktivet. Handlingsplanen omsätter strategin i konkret handling genom aktiviteter i form av bland annat specifika uppdrag och styrning av myndigheter. Utvärdering och revidering av handlingsplanens innehåll kommer att ske på det sätt som regeringen ser behov av. Handlingsplanens innehåll kommer att uppdateras löpande och aktiviteter tillföras för att stegvis uppnå målen.

betyder ansvarig utförare för aktiviteten[1].

betyder tidsperiod för åtgärdens genomförande.

1 Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

Pelare A: Systematiskt och effektivt cybersäkerhetsarbete

Mål 1: Ökat cybersäkerhetsarbete hos privata och offentliga organisationer

1.1 Nationellt cybersäkerhetscenter (NCSC) verksamhet inom Försvarets radioanstalt (FRA) bedrivs utifrån en ny förordning

Syfte: Att ge tydlig och långsiktig styrning som lägger grunden för ett välfungerande NCSC och tydliggör dess roll i det nationella cybersäkerhetsarbetet.

Regeringen

Tills vidare

1.2 CER- och NIS 2-direktiven genomför nationellt på ett harmoniserat sätt

Syfte: Genom att, bland annat med stöd i slutsatserna och förslagen i betänkandena om genomförande av NIS 2- och CER-direktiven (SOU 2024:18 och 2024:64), stärka och harmonisera lagstiftningen på området skapas förutsättningar för att cybersäkerhetsarbetet hos organisationer ska få större genomslag samt bidra till ökad motståndskraft i samhällsviktig verksamhet och därmed ett stärkt civilt försvar.

Regeringen

2025

1.3 En särskild utredare ska analysera behovet av och föreslå åtgärder och kompletterande författningsbestämmelser som behövs i syfte att anpassa svensk rätt till EU:s cyberresiliensförordning (CRA)

Syfte: Att bland annat analysera vilka svenska regelverk som berörs, föreslå sanktionsbestämmelser samt vilken eller vilka myndigheter som bör bli nationell marknadskontrollmyndighet och anmälande myndighet.

Fi 2024:07

2025

1.4 Myndigheten för samhällsskydd och beredskap (MSB) säkerställer att utbildningar kommer till stånd för organisationer som omfattas av NIS 2-direktivet och beredskapssektorerna

Syfte: Aktiviteten stödjer målet genom att höja kompetensen hos organisationer som ska bedriva ett systematiskt cybersäkerhetsarbete.

MSB

2024–2027

1.5 FRA och MSB ska inom ramen för NCSC ta framriktlinjer för att främja utveckling och integrering av relevant avancerad teknik som syftar till att genomföra moderna riskhanteringsåtgärder för cybersäkerhet, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) kräver

Syfte: Aktiviteten stödjer målet genom att främja moderna cyberriskhanteringsåtgärder som en del i organisationers cybersäkerhetsarbete.

FRA och MSB med bistånd av Försvarets materielverk (FMV), Försvarsmakten, Polismyndigheten, Post- och telestyrelsen (PTS) och Säkerhetspolisen

2025–2026

1.6 MSB fortsätter utveckla och förvalta råd och stöd för organisationers systematiska cybersäkerhetsarbete

Syfte: Aktiviteten stödjer målet genom att organisationer kan få vägledning i sitt cybersäkerhetsarbete.

MSB

Tills vidare

1.7 MSB fortsätter arbetet med analyser och temarapporter inom cybersäkerhetsområdet

Syfte: Myndighetens arbete med analyser och temarapporter är till gagn för organisationers cybersäkerhetsarbete och arbetet med att stärka samhällets motståndskraft.

MSB

Tills vidare

1.8 Finansinspektionen fortsätter utöva tillsyn över den finansiella sektorns cybersäkerhetsarbete och digitala operativa motståndskraft

Syfte: Genom tillsyn säkerställer Finansinspektionen att den finansiella sektorn (som består i huvudsak av privata aktörer som tillhandahåller tjänster som bland annat betalningsförmedling och kapitalförvaltning) upprätthåller en hög nivå av cybersäkerhetsarbete och digital motståndskraft i enlighet med DORA-förordningens krav.

Finansinspektionen

Tills vidare

1.9 MSB vidareutvecklar Cybersäkerhetskollen för att kunna bistå fler organisationer i fler processer och kunna förmedla en fördjupad nationell lägesbild kring cybersäkerhetsnivån i samhällsviktiga verksamheter

Syfte: Genom att utöka Cybersäkerhetskollen med stöd för bedömning av organisationens it- och OT-säkerhet samt leveranskedjor får organisationer ett ändamålsenligt verktyg att både bedöma sin nivå inom flera centrala områden samt förslag på åtgärder för att hantera identifierade brister. Utvecklingen ger även tillgång till en bredare och mer fördjupad lägesbild som stöd för riktade insatser på nationell nivå.

MSB

2025–2027

Mål 2: Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering

2.1 MSB tillförs medel för förberedelse av en nationell kartläggning av kommuners tekniska cybersäkerhetsförmåga

Syfte: Förbereda en nationell kartläggning av små och medelstora aktörer för att få en överblick över den tekniska cybersäkerhetsförmågan hos målgruppen.

MSB

2025–2027

2.2 Över 100 myndigheter implementerar uppdrag att redogöra för hur de förvaltat och utvecklat sitt arbete med informations- och cybersäkerhet

Syfte: Att skärpa myndigheternas återrapporteringskrav och prioriterar arbetet inom informations- och cybersäkerhet och ger regeringen underlag för ytterligare åtgärder på området.

Berörda statliga myndigheter

2025–2026

2.3 MSB etablerar en kompletterande analysmiljö till Cybersäkerhetskollen där drift, förvaltning och utveckling ingår

Syfte: Aktiviteten stödjer målet genom utveckling av verktyget och därmed ökade förutsättningar för samhällsviktiga verksamheter att nyttja det för att nå en tillfredställande cybersäkerhetsnivå.

MSB

2025–2027

2.4 FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för att inkludera och specificera cybersäkerhetsrelaterade krav för IKT-produkter och IKT-tjänster vid offentlig upphandling, inbegripet vad gäller cybersäkerhetscertifiering, kryptering och användning av cybersäkerhetsprodukter med öppen källkod, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) anger att medlemsstaterna ska anta

Syfte: Att erbjuda vägledning avseende säkrare upphandling vilket är av särskild vikt för att höja cybersäkerheten i statlig och kommunal förvaltning.

FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

2025–2026

2.5 Regeringskansliet uppdaterar strategins bilaga 2, ”Organisationer med roller och ansvarsområden inom cybersäkerhet”, när NIS 2-regleringen implementerats nationellt och definierat ansvarsförhållanden samt när uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (dir. 2024:111) redovisats och förslagen omhändertagits

Syfte: Aktiviteten stödjer målet genom att Regeringskansliet klargör hur ansvaret för det nationella cybersäkerhetsarbetet är fördelat.

Regeringskansliet

2025

2.6 Uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet

Syfte: Att stärka den nationella cybersäkerheten och motståndskraften genom en samlad och samordnad styrning av samhällets informations- och cybersäkerhetsarbete och en ändamålsenlig myndighetsstruktur.

Fö 2024:04

2024– 2025

Mål 3: Stärkt säkerhetsarbete inom kritisk infrastruktur

3.1 MSB tillhandahåller stöd för samhällsviktig verksamhets arbete med säkerhet i operativ teknik (OT)

Syfte: Aktiviteten stödjer målet genom att erbjuda operatörer stöd kring säkerhet i de OT-system som kritisk infrastruktur ofta är beroende av.

MSB

Tills vidare

3.2 FRA och MSB ska inom ramen för NCSC att ta fram riktlinjer för att upprätthålla den allmänna tillgängligheten, integriteten och konfidentialiteten hos den offentliga kärnan i det öppna internet, inbegripet, i tillämpliga fall, cybersäkerheten hos undervattenskablar, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) anger att medlemsstaterna ska anta

Syfte: Aktiviteten stödjer målet genom anpassade riktlinjer avseende säker och tillgänglig konnektivitet, vilket samhället är beroende av.

FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

2025–2026

3.3 Hotbildsstyrda penetrationstester genomförs regelbundet på organisationer inom den finansiella sektorn

Syfte: Hotbildsstyrda penetrationstester syftar till att en aktör inom den finansiella sektorn ska kunna bedöma sin beredskap att hantera it-incidenter, identifiera svagheter, brister och luckor i den digitala motståndskraften och snabbt genomföra korrigerande åtgärder. Enligt DORA-förordningen ska finansiella entiteter som har central betydelse för det finansiella systemet regelbundet genomföra sådana tester. Finansinspektionen beslutar om vilka entiteter som ska göra dessa tester och Riksbanken ska övervaka och samordna testerna.

Finansinspektionen och Sveriges Riksbank

Tills vidare

Mål 4: Robustare digitala leveranskedjor och minskat beroende

4.1 Berörda statliga myndigheter fortsätter inom ramen för etablerad NCSC-samordning kring standardisering av cybersäkerhet

Syfte: Att genom myndighetsgemensam samordning samverka frågor av myndighetsöverskridande relevans kring internationell standardisering på cybersäkerhetsområdet.

PTS och FMV i samverkan med Försvarsmakten, FRA, MSB, Säkerhetspolisen och Polismyndigheten

Tills vidare

4.2 FMV deltar i samarbeten och aktiviteter som bedrivs inom ramen för EU:s ramverk för cybersäkerhetscertifiering. I dessa sammanhang ska myndigheten bland annat söka få genomslag för svenska ståndpunkter och verka för att nya certifieringsordningar tas fram på ett transparent sätt

Syfte: Aktiviteten stödjer målet genom att transparenta och välanpassade certifieringsordningar kan användas för att höja cybersäkerhetsnivån för it-produkter, it-tjänster och relevanta processer.

FMV

Tills vidare

4.3 MSB genomför en kartläggning av digitala leveranskedjor och tar fram en modell för uppföljning av digitala leveranskedjor

Syfte: Att kartlägga digitala leveranskedjor inom vissa sektorer och identifiera särskilt skyddsvärda digitala leveranskedjor samt bedöma förekomsten av monoberoenden och kritiska beroenden till tredjeland. Därför syftar uppdraget till att möjliggöra framtagandet av en modell för uppföljning av digitala leveranskedjor som kompletterar den befintliga struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen som regeringen den 19 september 2019 uppdrog MSB att upprätta (Ju2019/03058/SSK och Ju2019/02421/SSK).

MSB

2025–2026

4.4 FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för cybersäkerhet i leveranskedjan för IKT-produkter och IKT-tjänster som används av entiteter när de tillhandahåller sina tjänster, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) anger att medlemsstaterna ska anta

Syfte: Aktiviteten stödjer målet genom att bidra till organisationers möjlighet att säkra sina leveranskedjor och därmed minska sin sårbarhet för cyberangrepp och störningar.

FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

2025–2026

Mål 5: Förenklad regelefterlevnad och stärkt funktionellt tillsynsarbete

5.1 MSB är nationell gemensam kontaktpunkt i enlighet med NIS-direktivet

Syfte: Aktiviteten stödjer målet genom att MSB i egenskap av kontaktpunkt bland annat bedriver tillsynssamordning via ett samarbetsforum för effektiv och likvärdig tillsyn kopplat till NIS-regleringen samt deltar i internationell samverkan rörande regulatoriska policyfrågor (Sveriges representant i NIS-Cooperation Group).

MSB

2025

5.2 Berörda statliga myndigheter fortsätter inom ramen för NCSC arbetet med en nationell modell där föreskrifter, allmänna råd och vägledningar så långt som möjligt ensas så att de följer en likartad logik, struktur och terminologi

Syfte: Aktiviteten stödjer målet genom att se över hur en samordnad regelutformning kan främja enklare regelefterlevnad, exempelvis genom myndighetsgemensam vägledning rörande it-säkerhetslösningar.

FRA, Försvarsmakten, MSB, Säkerhetspolisen och FMV

Tills vidare

5.3 Medel tillförs ett antal statliga myndigheter för att förbereda och utveckla sin tillsynsverksamhet utifrån NIS 2-direktivet

Syfte: Aktiviteten stödjer målet genom att skapa bättre förutsättningar för tillsynsmyndigheter att hantera de ökade kraven rörande tillsyn som följer av NIS 2-direktivet. Genom aktiviteten ges tillsynsverksamheten under NIS 2-direktivet goda förutsättningar från dag ett.

Vissa länsstyrelser, Läkemedelsverket, Inspektionen för vård och omsorg, Transportstyrelsen, Livsmedelsverket, Statens energimyndighet samt PTS

2025–2027

5.4 Säkerhetspolisen och Försvarsmakten utvecklar löpande tillsynsverksamheten kring, och samarbetet mellan myndigheter som har ansvar enligt, säkerhetsskyddslagstiftningen

Syfte: Aktiviteten stödjer målet genom att ändamålsenlig tillsyn kan bidra till bland annat cybersäkerheten i samhället.

Säkerhetspolisen och Försvarsmakten

Tills vidare

5.5 Säkerhetspolisen och Försvarsmakten utvecklar kontinuerligt stödjande material såsom vägledningar, handböcker och utbildningsmaterial inom säkerhetsskydd

Syfte: Aktiviteten bidrar till att förenkla regelefterlevnaden för aktörer som träffas av cybersäkerhetskrav inom ramen för bland annat säkerhetsskyddsregleringen.

Säkerhetspolisen och Försvarsmakten

Tills vidare

5.6 MSB förvaltar, utvecklar och tillhandahåller publik databas över svensk terminologi inom cybersäkerhetsområdet

Syfte: Att säkerställa en ensad terminologi som förenklar organisationers cybersäkerhetsarbete och samarbete sinsemellan.

MSB

Tills vidare

5.7 MSB tillhandahåller och vidareutvecklar rådgivningstjänst med särskilt fokus på NIS 2-aktörer

Syfte: Genom aktiviteten erbjuds verksamhetsutövare rådgivning som stöd för organisationers anpassning till att efterleva NIS 2-direktivets krav.

MSB

2025–2027

Mål 6: Utvecklat stöd för små och medelstora företags cybersäkerhetsarbete

6.1 FRA och MSB ska inom ramen för NCSC ta fram riktlinjer som stärker cyberresiliensen och cyberhygienen hos små och medelstora företag, särskilt de som inte omfattas av NIS 2-direktivet, genom att tillhandahålla lättillgänglig vägledning och stöd för deras specifika behov, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) anger att medlemsstaterna ska anta

Syfte: Aktiviteten stödjer målet genom att ta fram riktlinjer som kan vara till gagn för små och medelstora företag som utvecklar sitt cybersäkerhetsarbete.

FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

2025–2026

6.2 Medel tillförs MSB för att intensifiera det brottsförebyggande samarbetet med Stöldskyddsföreningen

Syfte: Genom att vidareutveckla arbetet med målgruppsanpassat stöd förstärks stödet till små och medelstora företag ytterligare.

MSB

2025–2027

Pelare B: Utvecklad kunskap och kompetensutveckling inom cybersäkerhet

Mål 7: Ökad cybersäkerhetsmedvetenhet och cyberhygien hos allmänheten

7.1 Medel tillförs MSB för att vidareutveckla kampanjen ”Tänk säkert”

Syfte: Aktiviteten stödjer målet genom att kampanjen syftar till att öka cybersäkerhetsmedvetenhetenen i samhället vilket långsiktigt bidrar till att höja lägstanivån och därmed motståndskraften mot såväl cyberattacker som andra hybridaktiviteter.

MSB

2025–2027

Mål 8: Stärkt kompetensförsörjning, utbildning och fortbildning inom cybersäkerhet

8.1 Medel tillförs Cybercampus Sverige för att ytterligare stärka verksamheten

Syfte: Aktiviteten stödjer målet genom att ge Cybercampus ökade förutsättningar att utgöra navet för utbildning, forskning och kompetensförsörjning inom hela cybersäkerhetsområdet.

Cybercampus vid Kungliga Tekniska högskolan

2024–2028

8.2 Försvarsmakten, Säkerhetspolisen och Försvarshögskolan samarbetar kring kompetensförsörjning inom primärt säkerhetsskyddsområdet

Syfte: Aktiviteten stödjer målet genom ett stärkt samarbete mellan aktörer som syftar till att avhjälpa brister i kompetensförsörjning på säkerhetsområdet.

Försvarsmakten, Säkerhetspolisen samt Försvarshögskolan

Tills vidare

8.3 MSB fortsätter arbetet med kompetensförsörjning inom cybersäkerhet

Syfte: Att stödja och sammanlänka med det arbete som sker på EU-nivå i europeiska kompetenscentrumet för cybersäkerhet (ECCC) rörande standardiserade roller, profiler och kompetenser inom cybersäkerhet.

MSB

Tills vidare

8.4 Mediemyndigheten fortsätter verka för medie- och informationskunnighet (MIK) och att samordna det nationella arbetet med MIK

Syfte: Myndigheten har i uppgift att verka för MIK och att samordna arbetet med MIK i Sverige. De koordinerar ett nätverk bestående av 24 myndigheter och organisationer samt fyra kretsar för samverkan - Folkbildningsarenan för MIK, Interregionala MIK-nätverket, Akademiskt forum för MIK-forskning samt Mediearenan för MIK. Syftet med nätverket är att genom samverkan utveckla kunskap, stärka kvaliteten och effektivisera arbetet – och därigenom stärka medie- och informationskunnigheten hos alla i Sverige. Det är ett område i utveckling, eftersom teknik och medieanvändning ständigt förändras. Inom nätverket ansvarar myndigheten även för en kunskapsbank om MIK med informationsmaterial, forskningsrapporter och lärarhandledningar från olika verksamheter som är tillgängligt för alla.

Mediemyndigheten

Tills vidare

8.5 FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för att främja och utveckla cybersäkerhetsutbildning, cybersäkerhetskompetens, medvetandehöjande åtgärder och forsknings- och utvecklingsinitiativ, samt vägledning om god praxis och kontroll för cyberhygien som riktar sig till medborgare, intressenter och entiteter, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) anger att medlemsstaterna ska anta

Syfte: Aktiviteten stödjer målet genom att riktlinjer upprättas som bland annat berör centrala frågor för att främja ökad cybersäkerhetskompetens.

FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

2025–2026

Mål 9: Stärkt forskning och innovation på cybersäkerhetsområdet

9.1 MSB tillhandahåller ett nationellt samordningscenter (NCC-SE)

Syfte: NCC-SE stöttar EU:s kompetenscentrum för cybersäkerhet (ECCC), bidrar i framtagning av arbetsprogram på EU-nivå, marknadsför de europeiska cybersäkerhetsutlysningarna samt ger vägledning till svenska aktörer som söker EU-medel för projekt inom arbetsprogrammen från ECCC. Sammantaget bidrar aktiviteten till målet genom att ge förutsättning för stärkt forskning och innovation.

MSB

Tills vidare

9.2 Medel tillförs för stärkt forskning och innovation inom cybersäkerhet genom nationellt samordningscenter (NCC-SE)

Syfte: Genom att stärka NCC-SE, inklusive dess möjlighet att förvalta EU-medel som stöd till tredje part, ökas förutsättningarna för stärkt forskning och innovation på cybersäkerhetsområdet i Sverige.

MSB

2025–2027

9.3 Medel tillförs för MSB:s vidareutveckling av Cybernoden

Syfte: Aktiviteten stödjer målet genom att den svenska Cybernodens arbete med att samla näringsliv, akademi och offentlig sektor utvecklas.

MSB

2025–2027

9.4 MSB beställer, kvalitetssäkrar och förmedlar forskning och utvecklingsarbete för informations- och cybersäkerhet

Syfte: Aktiviteten stödjer målet genom att MSB, inom ramen för myndighetens utlysningar inom samhällsskydd och beredskap, också främjar forskning på cybersäkerhetsområdet.

MSB

Tills vidare

9.5 Medel tillförs Vetenskapsrådet för satsningar inom ett antal forskningsområden

Syfte: Att stärka forskningen genom program inom:

- informations- och cybersäkerhet,
- digitaliseringens samhälleliga konsekvenser, och
- säkra samhällen.

Vetenskapsrådet

2025

Mål 10: Stärkt förmåga att hantera framväxande teknologiers risker och möjligheter

10.1 Uppdrag till Mediemyndigheten att genomföra en nationell satsning för stärkt medie- och informationskunnighet i en tid av artificiell intelligens och desinformation

Syfte: Aktiviteten stödjer målet genom att stärka individer som medvetna medieanvändare och även höja befolkningens kunskap om AI.

Mediemyndigheten

2024–2025

10.2 Regeringen gör en satsning som uppgår till drygt 1,2 miljarder kronor årligen från 2028 på excellenskluster för banbrytande teknik

Syfte: Kvantteknik har potentialen att revolutionera databehandling, simulering, sensorer och kommunikation och lösa problem som dagens datorer inte kan hantera. Denna breda satsning syftar till att täcka in såväl forskning på teknik i ett tidigt skede som innovation och tillämpning i ett senare skede av teknikutvecklingen och går därför via både Vetenskapsrådet och Vinnova.

Vetenskapsrådet och Vinnova

2024–2028

10.3 Försvarsmakten deltar i samarbete och aktiviteter som bedrivs inom EU:s och Natos arbetsgrupper för krypto och relevanta standardiseringsforum. I dessa sammanhang ska myndigheten bland annat söka få genomslag för svenska ståndpunkter och verka för att policy och regelverk är praktiskt genomförbart, ger ett adekvat skydd och tar hänsyn till kvantdatorhotet

Syfte: Aktiviteten stödjer målet genom att söka öka svensk förmåga att hantera risker kopplade till framtida kvantutveckling och kvantdatorer.

Försvarsmakten med stöd av FRA

Tills vidare

10.4 Försvarsmakten undersöker förutsättningarna för att anpassa krav och utveckling av kommande signalskyddssystem efter Natos policy, krav och interoperabilitetsspecifikationer

Syfte: Aktiviteten stödjer målet genom att bidra till utvecklad svensk kompetens och förmåga inom signalskydd.

Försvarsmakten

Tills vidare

Pelare C: Förmåga att förhindra och hantera cybersäkerhetsincidenter

Mål 11: Effektivare och säkrare informationsdelning nationellt och internationellt

11.1 FRA ska inom ramen för NCSC främja samverkan med privata och offentliga aktörer

Syfte: Stärkt privat-offentlig samverkan skapar förutsättningar för bland annat effektivare informationsdelning.

FRA i samverkan med FMV, Försvarsmakten, MSB, Polismyndigheten, PTS och Säkerhetspolisen

Tills vidare

11.2 NCSC tar fram lägesbilder avseende cyberhot och incidenter

Syfte: Aktiviteten stödjer målet genom att lägesbilder avseende aktuella cyberhot och incidenter tas fram för näringslivet, kommuner och regioner, myndigheter samt Regeringskansliet och därmed stöttar aktörer i att förstå hotbilden på såväl cyber- som hybridområdet.

FRA i samverkan med FMV, Försvarsmakten, MSB, Polismyndigheten, PTS och Säkerhetspolisen

Tills vidare

11.3 FRA och MSB ska inom ramen för NCSC ta fram riktlinjer inbegripet relevanta förfaranden och lämpliga verktyg för informationsutbyte för att stödja ett frivilligt informationsutbyte om cybersäkerhet mellan entiteter i enlighet med unionsrätten, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) kräver

Syfte: Riktlinjer rörande frivilligt informationsutbyte om cybersäkerhet bidrar till effektiv informationsdelning.

FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

2025–2026

11.4 FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för hantering av sårbarheter, inbegripet främjande och underlättande av samordnad delgivning av information om sårbarheter enligt NIS 2-direktivets artikel 12.1, som en del i att fastställa de riktlinjer som direktivets artikel 7.2 a) - j) kräver

Syfte: Aktiviteten stödjer målet genom att adressera delning av information om sårbarheter, vilket utgör en viktig aspekt av effektiv informationsdelning.

FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

2025–2026

11.5 Berörda statliga myndigheter fortsätter att inom ramen för årsrapporter informera om hotbilden inom sina respektive sakområden

Syfte: Myndigheternas olika perspektiv i rapporterna stödjer målet genom att utgöra ett viktigt bidrag i informationsdelning från statliga myndigheter som organisationer kan nyttja för att skapa sig en god lägesbild.

FRA, Försvarsmakten, MSB, Säkerhetspolisen, Polismyndigheten, FMV och PTS

2025–2026

Mål 12: Stärkt privat-offentlig hantering av cybersäkerhetsincidenter

12.1 FRA fortsätter erbjuda tekniskt detekterings- och varningssystem (TDV) till de mest skyddsvärda verksamheterna

Syfte: Genom att utveckla och tillhandahålla TDV stärks de mest skyddsvärda verksamheternas förmåga att förebygga och upptäcka cybersäkerhetsincidenter.

FRA

Tills vidare

12.2 Nationell informationssäkerhetsövning (NISÖ) fortsätter att genomföras inom ramen för NCSC

Syfte: Aktiviteten stödjer målet genom att ge privata och offentliga aktörer möjlighet att öva tillsammans och därigenom stärka samhällets samlade förmåga att hantera it-relaterade samhällsstörningar där skyndsam samordning krävs.

MSB i samverkan med berörda aktörer

Tills vidare

12.3 Statliga myndigheter genomför inom ramen för NCSC nationella cybersäkerhetsövningar

Syfte: Aktiviteten stödjer målet genom övningar som bland annat berör incidenthantering och bidrar till att stärka Sveriges förmåga att förebygga, upptäcka och hantera cyberhot och cyberangrepp.

FRA i samverkan med FMV, Försvarsmakten, MSB, Polismyndigheten, PTS och Säkerhetspolisen

Tills vidare

12.4 MSB fortsätter att planera, genomföra, utvärdera cybersäkerhetsövningar, inklusive att utveckla nationell Cyber Range

Syfte: Genom att stärka det kollektiva lärandet höjs privata och offentliga organisationers incidenthanteringsförmåga.

MSB

Tills vidare

12.5 MSB skapar en samlad portal med smarta formulär för rapportering av incidenter, tillbud, sårbarheter och cyberhot under olika regelverk, primärt NIS 2- och CER-direktivet

Syfte: Att förenkla organisationers cybersäkerhetsincidenthanteringsarbete genom att:

- undanröja krav på duplicerad NIS 2- och CER-rapportering, och
- införa möjlighet till ökat informationsutbyte och ytterligare funktionalitet för både rapporterande och mottagande organisationer.

Genom framtida planerad utveckling av portalen väntas också förbättrade möjligheter till informationsdelning och samverkan mellan mottagande statliga myndigheter och andra statliga myndigheter som ytterligare leder till att stärka det nationella incidenthanteringsarbetet.

MSB

Tills vidare

12.6 MSB fortsätter arbetet med årsrapporter om it-incidenter

Syfte: Aktiviteten stödjer målet genom att incidenter som rapporterats in till den statliga myndigheten sammanställs och analyseras över tid vilket möjliggör att följa trender kring cybersäkerhetsincidenter samt för organisationer att dra lärdomar till sin incidenthanteringsförmåga.

MSB

Tills vidare

12.7 FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för att främja ett aktivt cyberskydd, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) kräver

Syfte: Aktiviteten stödjer målet genom att främja ett aktivt cyberskydd, vilket organisationer kan använda för att stärka sin förmåga att hantera och bemöta cybersäkerhetsincidenter.

FRA och MSB med bistånd av FMV, Försvarsmakten, MSB, Polismyndigheten, PTS och Säkerhetspolisen

2025–2026

12.8 Polismyndigheten ser över förutsättningarna att etablera en process för ökat samarbete kring incidentrapportering

Syfte: Aktiviteten stödjer målet genom att se över förutsättningarna att mer effektivt nyttja statliga myndigheters samlade utredande, hanterande och förebyggande resurser på cybersäkerhetsområdet för att förebygga eller lagföra cyberbrott.

Polismyndigheten

Tills vidare

12.9 Inom ramen för NTSG:s krisberedskapsövningar övar aktörer inom elektroniska kommunikationer på cyberincidenter när så är lämpligt

Syfte: Aktörer inom elektronisk kommunikation utvecklar bättre rutiner och färdigheter i hanteringen av cybersäkerhetsrelaterade risker.

PTS

Tills vidare

12.10 FRA ska utarbeta en nationell operativ plan för storskaliga cybersäkerhetsincidenter och kriser i enlighet med artikel 9 i NIS 2-direktivet

Syfte: En operativ plan om storskaliga incidenter och kriser är en central del i att utveckla Sveriges samlade förmåga att snabbt och effektivt kunna hantera sådana incidenter och kriser.

MSB och FRA

2025

12.11 MSB är cyberkrishanteringsmyndighet med ansvar för att samordna hanteringen av storskaliga cybersäkerhetsincidenter och kriser enligt artikel 9.1 och CSIRT-enhet enligt artikel 10.1 NIS 2-direktivet

Syfte: Att utse behörig myndighet med ansvar för vissa uppgifter enligt NIS 2-direktivet.

MSB

2025

12.12 Medel tillförs MSB för utveckling av stärkt operativ cybersäkerhetsförmåga

Syfte: Att stärka funktionen CERT-SE och utveckla förmågan att erbjuda kvalificerat stöd till drabbade aktörer samt fortsätta att bygga förmåga att hantera cyberangrepp.

MSB

2025–2027

12.13 MSB verkar för att privata och offentliga organisationer ges tillgång till och kan nyttja det tekniska och organisatoriska stöd som tillhandahålls på EU-nivå för att stärka motståndskraften mot storskaliga cyberattacker

Syfte: Att dra nytta av det stöd som bland annat ENISA tillhandahåller i syfte att stärka organisationers möjlighet att förebygga och hantera storskaliga cyberattacker.

MSB

Tills vidare

Mål 13: Utvecklad förmåga att förebygga och bekämpa cyberbrott

13.1 Polismyndigheten fortsätter att fördjupa sitt samarbete med andra säkerhets- och brottsbekämpande myndigheter samt relevanta privata aktörer

Syfte: Aktiviteten stödjer målet genom operativt samarbete som ökar förmågan att bekämpa cyberbrott.

Polismyndigheten

Tills vidare

13.2 MSB är nationell gemensam kontaktpunkt i enlighet med NIS-direktivet

Syfte: Genom rollen som nationell gemensam kontaktpunkt bidrar MSB till målet genom att bland annat säkerställa samarbete mellan brottsbekämpande myndigheter och dataskyddsmyndigheter.

MSB

2025

13.3 Polismyndigheten deltar i samarbete med finans- och transaktionsmarknaderna i arbetet för säkrare betalningar

Syfte: Att förebygga cyberbrott inom transaktionssystemen.

Polismyndigheten

Tills vidare

13.4 Polismyndigheten deltar i brottsförebyggande nätverk gällande cyberbrott

Syfte: Att genom bred samverkan öka förmågan att förebygga cyberbrott.

Polismyndigheten

Tills vidare

13.5 Polismyndigheten deltar i brottsförebyggande samarbete med Stöldskyddsföreningen och andra aktörer. Arbetet innefattar att genom Säkerhetskollen.se ge varningar till allmänheten om pågående bedrägeritrender, att via ett kunskapscenter med MSB och flera andra statliga myndigheter skapa bl.a. medvetandehöjande kampanjer och helpdesk samt att genom Digitala varningsgruppen fortsätta det brottsförebyggande arbetet

Syfte: Att genom samarbete stärka förutsättningarna att skydda allmänheten samt små och medelstora företag och därigenom öka förmågan att förebygga och bekämpa cyberbrott.

Polismyndigheten, MSB och Stöldskyddsföreningen

Tills vidare

13.6 Polismyndigheten fördjupar fortsatt samarbetet med Europol avseende brottsförebyggande arbete

Syfte: Genom ökad användning av det material och de aktiviteter som Europol erbjuder, bland annat under European Cyber Security Month (ECSM), bidrar aktiviteten till arbetet med att förebygga cyberbrott.

Polismyndigheten

Tills vidare

13.7 Polismyndigheten deltar fortsatt i Europols Joint Cybercrime Action Taskforce

Syfte: Aktiviteten stödjer målet genom att fördjupa det internationella samarbetet med statliga myndigheter och privata aktörer avseende utredning av cyberbrott.

Polismyndigheten

Tills vidare

13.8 Polismyndigheten utvecklar sin förmåga att bekämpa cyberbrott

Syfte: Aktiviteten stödjer målet genom att öka förmågan att utreda inträffade cyberbrott samt förmågan att säkra bevismaterial i digitala miljöer.

Polismyndigheten

Tills vidare

Förteckning över åtgärder

Här följer en överskådlig lista på samtliga åtgärder i handlingsplanen.

Pelare A: Systematiskt och effektivt cybersäkerhetsarbete

Mål 1: Ökat cybersäkerhetsarbete hos privata och offentliga organisationer

#	Åtgärd	Ansvarig	Tid	Styrmedel
1.1	Nationellt cybersäkerhets-center (NCSC) verksamhet inom Försvarets radioanstalt (FRA) bedrivs utifrån en ny förordning	Regeringen	Tills vidare	Förordning om det nationella cybersäkerhetscentret vid Försvarets radioanstalt
1.2	CER- och NIS 2-direktiven genomförs nationellt på ett harmoniserat sätt	Regeringen	2025	Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (CER-direktivet)
1.3	En särskild utredare ska analysera behovet av och föreslå åtgärder och kompletterande författnings-bestämmelser som behövs i syfte att anpassa svensk rätt till EU:s cyberresiliens-förordning (CRA)	Fi 2024:07	2025	Dir 2024:119
1.4	Myndigheten för samhällsskydd och beredskap (MSB) säkerställer att utbildningar kommer till stånd för organisationer som omfattas av NIS 2-direktivet och beredskapssektorerna	MSB	2024–2027	Budgetpropositionen 2025
1.5	FRA och MSB ska inom ramen för NCSC ta framriktlinjer för att främja utveckling och integrering av relevant avancerad teknik som syftar till att genomföra moderna riskhanteringsåtgärder för cybersäkerhet, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) kräver	FRA och MSB med bistånd av Försvarets materielverk (FMV), Försvarsmakten, Polismyndigheten, Post- och telestyrelsen (PTS) och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)

1.5	FRA och MSB ska inom ramen för NCSC ta framriktlinjer för att främja utveckling och integrering av relevant avancerad teknik som syftar till att genomföra moderna riskhanteringsåtgärder för cybersäkerhet, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) kräver	FRA och MSB med bistånd av Försvarets materielverk (FMV), Försvarsmakten, Polismyndigheten, Post- och telestyrelsen (PTS) och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)
1.6	MSB fortsätter utveckla och förvalta råd och stöd för organisationers systematiska cybersäkerhetsarbete	MSB	Tills vidare	Förordning med instruktion för MSB
1.7	MSB fortsätter arbetet med analyser och temarapporter inom cybersäkerhetsområdet	MSB	Tills vidare	Förordning med instruktion för MSB EU-finansierat projekt ENIAC
1.8	Finansinspektionen fortsätter utöva tillsyn över den finansiella sektorns cybersäkerhetsarbete och digitala operativa motståndskraft	Finansinspektionen	Tills vidare	Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA)
1.9	MSB vidareutvecklar Cybersäkerhetskollen för att kunna bistå fler organisationer i fler processer och kunna förmedla en fördjupad nationell lägesbild kring cybersäkerhetsnivån i samhällsviktiga verksamheter	MSB	2025–2027	Budgetpropositionen 2025

Mål 2: Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering

#	Åtgärd	Ansvarig	Tid	Styrmedel
2.1	MSB tillförs medel för förberedelse av en nationell kartläggning av kommuners tekniska cybersäkerhetsförmåga	MSB	2025–2027	Budgetpropositionen 2025
2.2	Över 100 myndigheter implementerar uppdrag att redogöra för hur de förvaltat och utvecklat sitt arbete med informations- och cybersäkerhet	Berörda statliga myndigheter	2025–2026	Regleringsbrev
2.3	MSB etablerar en kompletterande analysmiljö till Cybersäkerhetskollen där drift, förvaltning och utveckling ingår	MSB	2025–2027	Budgetpropositionen 2025

2.4	FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för att inkludera och specificera cybersäkerhetsrelaterade krav för IKT-produkter och IKT-tjänster vid offentlig upphandling, inbegripet vad gäller cybersäkerhetscertifiering, kryptering och användning av cybersäkerhetsprodukter med öppen källkod, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) anger att medlemsstaterna ska anta	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/000389)
2.5	Regeringskansliet uppdaterar strategins bilaga 2, ”Organisationer med roller och ansvarsområden inom cybersäkerhet”, när NIS 2-regleringen implementerats nationellt och definierat ansvarsförhållanden samt när uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (dir. 2024:111) redovisats och förslagen omhändertagits	Regeringskansliet	2025	NIS 2-direktivet
2.6	Uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet	Fö 2024:04	2024–2025	Dir. 2024:111

Mål 3: Stärkt säkerhetsarbete inom kritisk infrastruktur

#	Åtgärd	Ansvarig	Tid	Styrmedel
3.1	MSB tillhandahåller stöd för samhällsviktig verksamhets arbete med säkerhet i operativ teknik (OT)	MSB	Tills vidare	Förordning med instruktion för MSB
3.2	FRA och MSB ska inom ramen för NCSC att ta fram riktlinjer för att upprätthålla den allmänna tillgängligheten, integriteten och konfidentialiteten hos den offentliga kärnan i det öppna internet, inbegripet, i tillämpliga fall, cybersäkerheten hos undervattenskablar, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) anger att medlemsstaterna ska anta	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/000389)

3.3	Hotbildsstyrda penetrationstester genomförs regelbundet på organisationer inom den finansiella sektorn	Finansinspektionen och Sveriges Riksbank	Tills vidare	Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn Lag (2024:1278) med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn

Mål 4: Robustare digitala leveranskedjor och minskat beroende

#	Åtgärd	Ansvarig	Tid	Styrmedel
4.1	Berörda statliga myndigheter fortsätter inom ramen för etablerad NCSC-samordning kring standardisering av cybersäkerhet	PTS och FMV i samverkan med Försvarsmakten, FRA, MSB Säkerhetspolisen och Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter
4.2	FMV deltar i samarbeten och aktiviteter som bedrivs inom ramen för EU:s ramverk för cybersäkerhets-certifiering. I dessa sammanhang ska myndigheten bland annat söka få genomslag för svenska ståndpunkter och verka för att nya certifieringsordningar tas fram på ett transparent sätt	FMV	Tills vidare	Lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt, Förordning (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt, Övergripande instruktion vid förhandling enligt det europeiska ramverket för cybersäkerhetscertifiering
4.3	MSB genomför en kartläggning av digitala leveranskedjor och tar fram en modell för uppföljning av digitala leveranskedjor	MSB	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:5 (Fö2025/000390)
4.4	FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för cybersäkerhet i leveranskedjan för IKT-produkter och IKT-tjänster som används av entiteter när de tillhandahåller sina tjänster, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) anger att medlemsstaterna ska anta	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/000389)

Mål 5: Förenklad regelefterlevnad och stärkt funktionellt tillsynsarbete

#	Åtgärd	Ansvarig	Tid	Styrmedel
5.1	MSB är nationell gemensam kontaktpunkt i enlighet med NIS-direktivet	MSB	2025	Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster
5.2	Berörda statliga myndigheter fortsätter inom ramen för NCSC arbetet med en nationell modell där föreskrifter, allmänna råd och vägledningar så långt som möjligt ensas så att de följer en likartad logik, struktur och terminologi	FRA, Försvarsmakten, MSB, Säkerhetspolisen, och FMV	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter
5.3	Medel tillförs ett antal statliga myndigheter för att förbereda och utveckla sin tillsynsverksamhet utifrån NIS 2-direktivet	Vissa länsstyrelser, Läkemedelsverket, Inspektionen för vård och omsorg, Transportstyrelsen, Livsmedelsverket, Statens energimyndighet samt PTS	2025–2027	Budgetpropositionen 2025
5.4	Säkerhetspolisen och Försvarsmakten utvecklar löpande tillsynsverksamheten kring, och samarbetet mellan myndigheter som har ansvar enligt, säkerhetsskydds-lagstiftningen	Säkerhetspolisen och Försvarsmakten	Tills vidare	Förordningar med myndigheternas instruktioner Säkerhetsskyddslag (2018:585) Säkerhetsskyddsförordning (2021:955)
5.5	Säkerhetspolisen och Försvarsmakten utvecklar kontinuerligt stödjande material såsom vägledningar, handböcker och utbildningsmaterial inom säkerhetsskydd	Säkerhetspolisen och Försvarsmakten	Tills vidare	Förordningar med myndigheternas instruktioner Säkerhetsskyddslag (2018:585) Säkerhetsskyddsförordning (2021:955)
5.6	MSB förvaltar, utvecklar och tillhandahåller publik databas över svensk terminologi inom cybersäkerhetsområdet	MSB	Tills vidare	Förordning med instruktion för MSB
5.7	MSB tillhandahåller och vidareutvecklar rådgivningstjänst med särskilt fokus på NIS 2-aktörer	MSB	2025–2027	Förordning med instruktion för MSB Budgetpropositionen 2025

Mål 6: Utvecklat stöd för små och medelstora företags cybersäkerhetsarbete

#	Åtgärd	Ansvarig	Tid	Styrmedel
6.1	FRA och MSB ska inom ramen för NCSC ta fram riktlinjer som stärker cyberresiliensen och cyberhygienen hos små och medelstora företag, särskilt de som inte omfattas av NIS 2-direktivet, genom att tillhandahålla lättillgänglig vägledning och stöd för deras specifika behov, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) anger att medlemsstaterna ska anta	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/000389)
6.2	Medel tillförs MSB för att intensifiera det brottsförebyggande samarbetet med Stöldskyddsföreningen	MSB	2025–2027	Budgetpropositionen 2025

Pelare B: Utvecklad kunskap och kompetensutveckling inom cybersäkerhet

Mål 7: Ökad cybersäkerhetsmedvetenhet och cyberhygien hos allmänheten

#	Åtgärd	Ansvarig	Tid	Styrmedel
7.1	Medel tillförs MSB för att vidareutveckla kampanjen ”Tänk säkert”	MSB	2025–2027	Budgetpropositionen 2025

Mål 8: Stärkt kompetensförsörjning, utbildning och fortbildning inom cybersäkerhet

#	Åtgärd	Ansvarig	Tid	Styrmedel
8.1	Medel tillförs Cybercampus Sverige för att ytterligare stärka verksamheten	Cybercampus vid Kungl. Tekniska högskolan	2024–2028	Budgetpropositionen 2024 Forskning och innovation för framtid, nyfikenhet och nytta (prop. 2024/25:60)
8.2	Försvarsmakten, Säkerhetspolisen och Försvarshögskolan samarbetar kring kompetensförsörjning inom primärt säkerhetsskyddsområdet	Försvarsmakten, Säkerhetspolisen samt Försvarshögskolan	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter
8.3	MSB fortsätter arbetet med kompetensförsörjning inom cybersäkerhet	MSB	Tills vidare	Förordning med instruktion för MSB
8.4	Mediemyndigheten fortsätter verka för medie- och informationskunnighet (MIK) och att samordna det nationella arbetet med MIK	Mediemyndigheten	Tills vidare	Förordning med instruktion för Mediemyndigheten

8.5	FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för att främja och utveckla cybersäkerhetsutbildning, cybersäkerhets-kompetens, medvetande-höjande åtgärder och forsknings- och utvecklingsinitiativ, samt vägledning om god praxis och kontroll för cyberhygien som riktar sig till medborgare, intressenter och entiteter, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) anger att medlemsstaterna ska anta	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/000389)

Mål 9: Stärkt forskning och innovation på cybersäkerhetsområdet

#	Åtgärd	Ansvarig	Tid	Styrmedel
9.1	MSB tillhandahåller ett nationellt samordnings-center (NCC-SE)	MSB	Tills vidare	Förordning med instruktion för MSB Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum
9.2	Medel tillförs för stärkt forskning och innovation inom cybersäkerhet genom nationellt samordnings-center (NCC-SE)	MSB	2025–2027	Budgetpropositionen 2025
9.3	Medel tillförs för MSB:s vidareutveckling av Cybernoden	MSB	2025–2027	Budgetpropositionen 2025
9.4	MSB beställer, kvalitetssäkrar och förmedlar forskning och utvecklingsarbete för informations- och cybersäkerhet	MSB	Tills vidare	Förordning med instruktion för MSB
9.5	Medel tillförs Vetenskapsrådet för satsningar inom ett antal forskningsområden	Vetenskapsrådet	2025	Forskning, frihet, framtid – kunskap och innovation för Sverige (prop. 2020/21:60) Myndighetens regleringsbrev

Mål 10: Stärkt förmåga att hantera framväxande teknologiers risker och möjligheter

#	Åtgärd	Ansvarig	Tid	Styrmedel
10.1	Uppdrag till Mediemyndigheten att genomföra en nationell satsning för stärkt medie- och informationskunnighet i en tid av artificiell intelligens och desinformation	Mediemyndigheten	2024-2025	Regeringsuppdrag den 14 mars 2024 (Ku2024/00419)

10.2	Regeringen gör en satsning som uppgår till drygt 1,2 miljarder kronor årligen från 2028 på excellenskluster för banbrytande teknik	Vetenskapsrådet och Vinnova	2024–2028	Forskning och innovation för framtid, nyfikenhet och nytta (prop. 2024/25:60)
10.3	Försvarsmakten deltar i samarbete och aktiviteter som bedrivs inom EU:s och Natos arbetsgrupper för krypto och relevanta standardiseringsforum. I dessa sammanhang ska myndigheten bland annat söka få genomslag för svenska ståndpunkter och verka för att policy och regelverk är praktiskt genomförbart, ger ett adekvat skydd och tar hänsyn till kvantdatorhotet	Försvarsmakten med stöd av FRA	Tills vidare	Uppgiften som kryptogodkännande myndighet (NCSA/CAA) Förordning med instruktion för Försvarsmakten
10.4	Försvarsmakten undersöker förutsättningarna för att anpassa krav och utveckling av kommande signalskyddssystem efter Natos policy, krav och interoperabilitets-specifikationer	Försvarsmakten	Tills vidare	Uppgiften som kryptogodkännande myndighet (NCSA/CAA) Förordning med instruktion för Försvarsmakten

Pelare C: Förmåga att förhindra och hantera cybersäkerhetsincidenter

Mål 11: Effektivare och säkrare informationsdelning nationellt och internationellt

#	Åtgärd	Ansvarig	Tid	Styrmedel
11.1	FRA ska inom ramen för NCSC främja samverkan med privata och offentliga aktörer	FRA i samverkan med FMV, Försvarsmakten, MSB, Polismyndigheten, PTS och Säkerhetspolisen	Tills vidare	Förordning om det nationella cybersäkerhetscentret vid Försvarets radioanstalt
11.2	NCSC tar fram lägesbilder avseende cyberhot och incidenter	FRA i samverkan med FMV, Försvarsmakten, MSB, Polismyndigheten, PTS och Säkerhetspolisen	Tills vidare	Förordning om det nationella cybersäkerhetscentret vid Försvarets radioanstalt
11.3	FRA och MSB ska inom ramen för NCSC ta fram riktlinjer inbegripet relevanta förfaranden och lämpliga verktyg för informationsutbyte för att stödja ett frivilligt informationsutbyte om cybersäkerhet mellan entiteter i enlighet med unionsrätten, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) kräver	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)

11.4	FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för hantering av sårbarheter, inbegripet främjande och underlättande av samordnad delgivning av information om sårbarheter enligt NIS 2-direktivets artikel 12.1, som en del i att fastställa de riktlinjer som direktivets artikel 7.2 a) - j) kräver	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)
11.5	Berörda statliga myndigheter fortsätter att inom ramen för årsrapporter informera om hotbilden inom sina respektive sakområden	FRA, Försvarsmakten, MSB, Säkerhetspolisen, Polismyndigheten, FMV och PTS	Tills vidare	Förordningar med myndigheternas instruktioner

Mål 12: Stärkt privat-offentlig hantering av cybersäkerhetsincidenter

#	Åtgärd	Ansvarig	Tid	Styrmedel
12.1	FRA fortsätter erbjuda tekniskt detekterings- och varningssystem (TDV) till de mest skyddsvärda verksamheterna	FRA	Tills vidare	Förordning med instruktion för FRA
12.2	Nationell informations-säkerhetsövning (NISÖ) fortsätter att genomföras inom ramen för NCSC	MSB i samverkan med berörda aktörer	Tills vidare	Förordning med instruktion för MSB
12.3	Statliga myndigheter genomför inom ramen för NCSC nationella cybersäkerhetsövningar	FRA i samverkan med FMV, Försvarsmakten, MSB, Polismyndigheten, PTS och Säkerhetspolisen	Tills vidare	Förordning om det nationella cybersäkerhetscentret vid Försvarets radioanstalt
12.4	MSB fortsätter att planera, genomföra, utvärdera cybersäkerhetsövningar, inklusive att utveckla nationell Cyber Range	MSB	Tills vidare	Förordning med instruktion för MSB
12.5	MSB skapar en samlad portal med smarta formulär för rapportering av incidenter, tillbud, sårbarheter och cyberhot under olika regelverk, primärt NIS 2- och CER-direktivet	MSB	Tills vidare	EU-finansierat projekt ENIAC
12.6	MSB fortsätter arbetet med årsrapporter om it-incidenter	MSB	Tills vidare	Förordning med instruktion för MSB
12.7	FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för att främja ett aktivt cyberskydd, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) kräver	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)

12.8	Polismyndigheten ser över förutsättningarna att etablera en process för ökat samarbete kring incidentrapportering	Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter
12.9	Inom ramen för NTSG:s krisberedskapsövningar övar aktörer inom elektroniska kommunikationer på cyberincidenter när så är lämpligt	PTS	Tills vidare	Proposition 2023/24:60 En telesamverkansgrupp för fredstida kriser och höjd beredskap
12.10	FRA ska utarbeta en nationell operativ plan för storskaliga cybersäkerhetsincidenter och kriser i enlighet med artikel 9 i NIS 2-direktivet	MSB och FRA	2025	Regeringsuppdrag den 27 februari 2025 Fö nr II:2 (Fö2025/00388)
12.11	MSB är cyberkrishanterings-myndighet med ansvar för att samordna hanteringen av storskaliga cybersäkerhetsincidenter och kriser enligt artikel 9.1 och CSIRT-enhet enligt artikel 10.1 NIS 2-direktivet	MSB	2025	Regeringsuppdrag den 27 februari 2025 Fö nr II:1 (Fö2025/00387)
12.12	Medel tillförs MSB för utveckling av stärkt operativ cybersäkerhetsförmåga	MSB	2025–2027	Budgetpropositionen 2025
12.13	MSB verkar för att privata och offentliga organisationer ges tillgång till och kan nyttja det tekniska och organisatoriska stöd som tillhandahålls på EU-nivå för att stärka motståndskraften mot storskaliga cyberattacker	MSB	Tills vidare	Förordning med instruktion för MSB Enisa Support Action

Mål 13: Utvecklad förmåga att förebygga och bekämpa cyberbrott

#	Åtgärd	Ansvarig	Tid	Styrmedel
13.1	Polismyndigheten fortsätter att fördjupa sitt samarbete med andra säkerhets- och brottsbekämpande myndigheter samt relevanta privata aktörer	Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter
13.2	MSB är nationell gemensam kontaktpunkt i enlighet med NIS-direktivet	MSB	2025	Förordning med instruktion för MSB Lagen om informations-säkerhet för samhällsviktiga och digitala tjänster (2018:1174) Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster
13.3	Polismyndigheten deltar i samarbete med finans- och transaktionsmarknaderna i arbetet för säkrare betalningar	Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter

13.4	Polismyndigheten deltar i brottsförebyggande nätverk gällande cyberbrott	Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter
13.5	Polismyndigheten deltar i brottsförebyggande samarbete med Stöldskyddsföreningen och andra aktörer. Arbetet innefattar att genom Säkerhetskollen.se ge varningar till allmänheten om pågående bedrägeritrender, att via ett kunskapscenter med MSB och flera andra statliga myndigheter skapa bl.a. medvetandehöjande kampanjer och helpdesk samt att genom Digitala varningsgruppen fortsätta det brottsförebyggande arbetet	Polismyndigheten, MSB och Stöldskydds-föreningen	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter Budgetpropositionen 2025
13.6	Polismyndigheten fördjupar fortsatt samarbetet med Europol avseende brottsförebyggande arbete	Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter
13.7	Polismyndigheten deltar fortsatt i Europols Joint Cybercrime Action Taskforce	Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter
13.8	Polismyndigheten utvecklar sin förmåga att bekämpa cyberbrott	Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter

Regeringskansliet
Växel: 08-405 10 00
www.regeringen.se