RÅDETS AFGØRELSE (FUSP) 2021/1026

af 21. juni 2021

til støtte for Organisationen for Forbud mod Kemiske Våbens (OPCW's) program for cybersikkerhed og cyberrobusthed og informationssikring inden for rammerne af gennemførelsen af EU's strategi mod spredning af masseødelæggelsesvåben

RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Union, særlig artikel 28, stk. 1, og artikel 31, stk. 1,

under henvisning til forslag fra Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik, og

ud fra følgende betragtninger:

(1) Det Europæiske Råd vedtog den 12. december 2003 EU's strategi mod spredning af masseødelæggelsesvåben (»EU's strategi«), hvis kapitel III indeholder en liste over foranstaltninger til bekæmpelse af en sådan spredning.

(2) EU's strategi understreger den centrale rolle, som konventionen om forbud mod udvikling, fremstilling, oplagring og anvendelse af kemiske våben og sådanne våbens tilintetgørelse (CWC) og Organisationen for Forbud mod Kemiske Våben (OPCW) spiller i bestræbelserne på at opnå en verden uden kemiske våben. EU's strategis målsætninger supplerer OPCW's målsætninger i forbindelse med denne organisations ansvar for gennemførelsen af CWC.

(3) Rådet vedtog den 22. november 2004 fælles aktion 2004/797/FUSP ([1]) om støtte til OPCW's aktiviteter. Nævnte fælles aktion blev ved sit udløb efterfulgt af Rådets fælles aktion 2005/913/FUSP ([2]), som blev efterfulgt af Rådets fælles aktion 2007/185/FUSP ([3]).

Fælles aktion 2007/185/FUSP blev efterfulgt af Rådets afgørelse 2009/569/FUSP ([4]), 2012/166/FUSP ([5]), 2013/726/FUSP ([6]), (FUSP) 2015/259 ([7]), (FUSP) 2017/2302 ([8]), (FUSP) 2017/2303 ([9]) og (FUSP) 2019/538 ([10]).

([1]) Rådets fælles aktion 2004/797/FUSP af 22. november 2004 om støtte til OPCW's aktiviteter inden for rammerne af gennemførelsen af EU's strategi mod spredning af masseødelæggelsesvåben (EUT L 349 af 25.11.2004, s. 63).

([2]) Rådets fælles aktion 2005/913/FUSP af 12. december 2005 om støtte til OPCW's aktiviteter inden for rammerne af gennemførelsen af EU's strategi mod spredning af masseødelæggelsesvåben (EUT L 331 af 17.12.2005, s. 34).

([3]) Rådets fælles aktion 2007/185/FUSP af 19. marts 2007 om støtte til OPCW's aktiviteter inden for rammerne af gennemførelsen af EU's strategi mod spredning af masseødelæggelsesvåben (EUT L 85 af 27.3.2007, s. 10).

([4]) Rådets afgørelse 2009/569/FUSP af 27. juli 2009 om støtte til OPCW's aktiviteter inden for rammerne af gennemførelsen af EU's strategi mod spredning af masseødelæggelsesvåben (EUT L 197 af 29.7.2009, s. 96).

([5]) Rådets afgørelse 2012/166/FUSP af 23. marts 2012 til støtte for Organisationen for Forbud mod Kemiske Våbens (OPCW's) aktiviteter inden for rammerne af gennemførelsen af EU's strategi mod spredning af masseødelæggelsesvåben (EUT L 87 af 24.3.2012, s. 49).

([6]) Rådets afgørelse 2013/726/FUSP af 9. december 2013 om støtte til UNSCR 2118 (2013) og OPCW's eksekutivråd EC-M-33/Dec 1 inden for rammerne af gennemførelsen af EU-strategien mod spredning af masseødelæggelsesvåben (EUT L 329 af 10.12.2013, s. 41).

([7]) Rådets afgørelse (FUSP) 2015/259 af 17. februar 2015 til støtte for Organisationen for Forbud mod Kemiske Våbens (OPCW's) aktiviteter inden for rammerne af gennemførelsen af EU's strategi mod spredning af masseødelæggelsesvåben (EUT L 43 af 18.2.2015, s. 14).

([8]) Rådets afgørelse (FUSP) 2017/2302 af 12. december 2017 til støtte for OPCW-aktiviteterne for at bistå med oprensningsarbejdet på det tidligere oplagringssted for kemiske våben i Libyen inden for rammerne af gennemførelsen af EU's strategi mod spredning af masseødelæggelsesvåben (EUT L 329 af 13.12.2017, s. 49).

([9]) Rådets afgørelse (FUSP) 2017/2303 af 12. december 2017 til støtte for den fortsatte gennemførelse af FN's Sikkerhedsråds resolution 2118 (2013) og OPCW-Eksekutivrådets afgørelse EC-M-33/DEC.1 om destruktion af Syriens kemiske våben inden for rammerne af gennemførelsen af EU's strategi mod spredning af masseødelæggelsesvåben (EUT L 329 af 13.12.2017, s. 55).

([10]) Rådets afgørelse (FUSP) 2019/538 af 1. april 2019 til støtte for Organisationen for Forbud mod Kemiske Våbens (OPCW's) aktiviteter inden for rammerne af gennemførelsen af EU's strategi mod spredning af masseødelæggelsesvåben (EUT L 93 af 2.4.2019, s. 3).

(4) Det er nødvendigt at videreføre denne intensive og målrettede bistand fra Unionen til OPCW som led i den aktive gennemførelse af kapitel III i EU's strategi.

(5) Der er behov for yderligere EU-støtte til OPCW's program for cybersikkerhed og cyberrobusthed og informationssikring med henblik på at øge OPCW's kapacitet til at opretholde et passende niveau af cybersikkerhed og cyberrobusthed i håndteringen af nuværende og nye cybersikkerhedsudfordringer —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

1. Med henblik på at sikre en umiddelbar og praktisk anvendelse af visse af elementerne i EU's strategi støtter Unionen et OPCW-projekt med følgende formål:

— opgradering af IKT-infrastrukturen i overensstemmelse med OPCW's institutionelle kontinuitetsramme med stærkt fokus på robusthed, og

— sikring af privilegeret adgangsstyring samt fysisk, logisk og kryptografisk informationsstyring og -adskillelse i alle OPCW's strategiske netværk og missionsnetværk.

2. I forbindelse med stk. 1 er de aktiviteter i OPCW-projektet, som EU støtter, og som overholder de i kapitel III i EU's strategi omhandlede foranstaltninger, følgende:

— ibrugtagning af et gunstigt miljø for igangværende cybersikkerheds- og cyberrobusthedstiltag inden for OPCW's operationer på flere lokaliteter

— udformning af en skræddersyet løsning til integration og konfiguration af systemer på stedet og cloud-baserede systemer med OPCW's IKT-systemer og løsninger vedrørende styring af privilegeret adgang (PAM), og

— iværksættelse og afprøvning af PAM-løsninger.

3. Bilaget indeholder en detaljeret beskrivelse af de i stk. 2 omhandlede aktiviteter i OPCW, som Unionen støtter.

Artikel 2

1. Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik (»HR«) er ansvarlig for gennemførelsen af denne afgørelse.

2. Den tekniske gennemførelse af det i artikel 1 omhandlede projekt varetages af OPCW's tekniske sekretariat (»det tekniske sekretariat«). Det udfører denne opgave under HR's ansvar og tilsyn. HR indgår med henblik herpå de nødvendige ordninger med det tekniske sekretariat.

Artikel 3

1. Det finansielle referencegrundlag for gennemførelsen af det i artikel 1 omhandlede projekt er på 2 151 823 EUR.

2. De udgifter, der finansieres over beløbet i stk. 1, forvaltes i overensstemmelse med de procedurer og regler, der gælder for Unionens almindelige budget.

3. Kommissionen overvåger, at de i stk. 2 omhandlede udgifter forvaltes korrekt. Med henblik herpå indgår Kommissionen den nødvendige aftale med det tekniske sekretariat. Det skal fremgå af denne aftale, at det tekniske sekretariat sørger for at synliggøre Unionens bidrag i en grad, der svarer til dets størrelse, og fastsætter særlige foranstaltninger, som gør det lettere at udvikle synergier og undgå overlapning af aktiviteter.

4. Kommissionen bestræber sig på at indgå den aftale, der er omhandlet i stk. 3, snarest muligt efter denne afgørelses ikrafttræden. Den underretter Rådet om eventuelle vanskeligheder i forbindelse med denne proces og om datoen for indgåelsen af aftalen.

Artikel 4

HR aflægger rapport til Rådet om gennemførelsen af denne afgørelse på grundlag af regelmæssige rapporter fra det tekniske sekretariat. HR-rapporterne skal danne udgangspunkt for Rådets evaluering. Kommissionen oplyser om de finansielle aspekter af det i artikel 1 omhandlede projekt.

Artikel 5

1. Denne afgørelse træder i kraft på dagen for vedtagelsen.

2. Denne afgørelse udløber 24 måneder efter indgåelsen af aftalen i artikel 3, stk. 3. Den udløber dog seks måneder efter ikrafttræden, hvis nævnte aftale ikke er indgået inden da.

Udfærdiget i Luxembourg, den 21. juni 2021.

På Rådets vegne
J. BORRELL FONTELLES
Formand

BILAG

PROJEKTDOKUMENT

1. Baggrund

OPCW er forpligtet til at opretholde en infrastruktur, der tillader informationssuverænitet på en måde, der står i et rimeligt forhold til privilegerede adgangsklassifikationer, passende håndteringsrutiner og eksisterende trusler, og samtidig fortsat er i stand til at forsvare sig mod nye risici. OPCW står fortsat konstant over for alvorlige og nye risici i forbindelse med cybersikkerhed og cyberrobusthed. OPCW er et mål for særdeles dygtige, ressourcestærke og motiverede aktører. Disse aktører vedbliver med hyppigt at angribe fortroligheden og integriteten af OPCW's informations- og infrastrukturaktiver. Som reaktion på de problemer, som de seneste cyberangreb, aktuelle politiske overvejelser og covid-19-krisen har understreget, og under hensyntagen til de unikke krav som følge af karakteren af OPCW's arbejde med at opfylde CWC's mandat er der et klart behov for væsentlige investeringer i teknisk kapacitet.

Under OPCW's særlige fond for cybersikkerhed, driftskontinuitet og fysisk infrastruktursikkerhed har OPCW udformet sit program for cybersikkerhed og cyberrobusthed og informationssikring (OPCW-programmet) med 47 aktiviteter med henblik på at tackle de cybersikkerhedsudfordringer, man har oplevet i den senere tid. OPCW-programmet er tilpasset bedste praksis, som fremmes af enheder såsom Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) eller ved hjælp af koncepter i forbindelse med det europæiske direktiv om net- og informationssikkerhed (NIS) vedrørende telekommunikation og forsvar. Samlet set omfatter OPCW-programmet følgende tematiske områder: klassificerede og uklassificerede netværk, politik og styring, afsløring og reaktion, operationer og vedligeholdelse samt telekommunikation. OPCW-programmet er grundlæggende udformet til at reducere mulighederne for, at angribere med tilstrækkelige ressourcer og/eller statsfinansierede angribere kan nå deres mål, og mindske risiciene fra både eksterne trusler og insidertrusler fra såvel et menneskeligt som et teknisk perspektiv. Unionens støtte er struktureret som et projekt med tre aktiviteter, der svarer til to af OPCW-programmets 47 aktiviteter.

2. Projektformål

Projektets overordnede formål er at sikre, at OPCW's sekretariat har kapacitet til at opretholde et passende niveau af cybersikkerhed og cyberrobusthed i håndteringen af tilbagevendende og nye cybersikkerhedsudfordringer i OPCW's hovedkvarter og hjælpefaciliteter for at opfylde OPCW's mandat og gennemføre CWC effektivt.

3. Mål

— Opgradering af IKT-infrastrukturen i overensstemmelse med OPCW's institutionelle kontinuitetsramme med stærkt fokus på robusthed

— Sikring af privilegeret adgangsstyring samt fysisk, logisk og kryptografisk informationsstyring og -adskillelse i alle strategiske netværk og missionsnetværk.

4. Resultater

De forventede resultater, som projektet bidrager til, er følgende:

— IKT-udstyr og -tjenester sørger for robust systempålidelighed (hybrid/geografisk redundans) og fremmer øget tilgængelighed af IKT-systemer og -tjenester til støtte for driftskontinuitet

— Minimering af enhver enkelt faktors eller persons evne til at skade fortroligheden og integriteten af oplysninger eller systemer i OPCW.

5. Aktiviteter

5.1. Aktivitet 1 — Ibrugtagning af et gunstigt miljø for igangværende cybersikkerheds- og cyberrobusthedstiltag inden for OPCW's operationer på flere lokaliteter

Denne aktivitet tilstræber at sikre et gunstigt miljø for en problemfri udrulning af OPCW's kontinuitetsplanlægning i forbindelse med cybersikkerhed og cyberrobusthed. Dette opnås ved at tage fat på infrastrukturopgraderinger — ny arkitektur og/eller arkivering for OPCW's driftskontinuitet på tværs af operationer på flere lokaliteter. Samtidig lettes og muliggøres integrationen af privilegeret adgangsstyring i processerne for kontinuitetsplanlægning og -reaktion yderligere.

5.2. Aktivitet 2 — Udformning af en skræddersyet løsning til integration og konfiguration af systemer på stedet og cloud-baserede systemer med OPCW's IKT-systemer og løsninger vedrørende styring af privilegeret adgang (PAM)

Denne aktivitet har fokus på at omsætte det gunstige miljø til en skræddersyet udformning for integration og konfiguration af systemer på stedet og cloud-baserede systemer med OPCW's IKT-systemer og PAM-løsninger. Dette forventes at øge effektiviteten af IKT-systeminfrastrukturen og føre til, at der udformes et integreret PAM-system for kritiske aktiver, der kan virke afskrækkende, afsløre og er i overensstemmelse med en tilsvarende kapacitet til at forfølge trusler.

5.3. Aktivitet 3 — Iværksættelse og afprøvning af PAM-løsninger.

Denne aktivitet bygger på den implementerede infrastruktur og PAM-løsningerne, der er udformet, så integration og konfiguration kan omsættes fra teori til praksis. Systemerne skal kortlægges, profileres og indbygges i eksisterende systemer, samtidig med at der tages hensyn til dermed forbundne politiske og menneskelige faktorer. Herefter vil OPCW's sekretariat kunne identificere og afhjælpe mangler i videst muligt omfang via en grundig afprøvning, som verificerer og sikrer systemets robusthed (alle nye systemer har en stærk autentificering for brugere og udstyr, passende informationsklassificering og -beskyttelse samt avanceret forebyggelse af datatab) under gennemførelsen og over tid.

6. Varighed

Den samlede anslåede varighed af gennemførelsen, der finansieres gennem dette projekt, forventes at være på højst 24 måneder.

7. Støttemodtagere

Projektstøttemodtagerne vil være personalet i OPCW's tekniske sekretariat, politiske organer, hjælpeorganer og CWC-interessenter, herunder deltagende stater.

8. EU's synlighed

OPCW træffer alle passende foranstaltninger ud fra rimelige sikkerhedshensyn for at gøre opmærksom på, at dette projekt er blevet finansieret af Unionen.