COUNCIL DECISION (CFSP) 2021/1026

of 21 June 2021

in support of the Cyber Security and Resilience and Information Assurance Programme of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the framework of the implementation of the EU Strategy against Proliferation of Weapons of Mass Destruction

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Articles 28(1) and 31(1) thereof,

Having regard to the proposal from the High Representative of the Union for Foreign Affairs and Security Policy,

Whereas:

(1) On 12 December 2003 the European Council adopted the EU Strategy against Proliferation of Weapons of Mass Destruction ('the EU Strategy'), Chapter III of which contains a list of measures to combat such proliferation.

(2) The EU Strategy underlines the crucial role of the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (CWC) and of the Organisation for the Prohibition of Chemical Weapons (OPCW) in creating a world free of chemical weapons. The objectives of the EU Strategy are complementary to those pursued by the OPCW in the context of its responsibility for the implementation of the CWC.

(3) On 22 November 2004 the Council adopted Joint Action 2004/797/CFSP ([1]) on support for OPCW activities. That Joint Action was followed on its expiry by Council Joint Action 2005/913/CFSP ([2]), which in turn was followed by Council Joint Action 2007/185/CFSP ([3]).

Joint Action 2007/185/CFSP was followed by Council Decisions 2009/569/CFSP ([4]), 2012/166/CFSP ([5]), 2013/726/CFSP ([6]), (CFSP) 2015/259 ([7]), (CFSP) 2017/2302 ([8]), (CFSP) 2017/2303 ([9]) and (CFSP) 2019/538 ([10]).

([1]) Council Joint Action 2004/797/CFSP of 22 November 2004 on support for OPCW activities in the framework of the implementation of the EU Strategy against Proliferation of Weapons of Mass Destruction (OJ L 349, 25.11.2004, p. 63).

([2]) Council Joint Action 2005/913/CFSP of 12 December 2005 on support for OPCW activities in the framework of the implementation of the EU Strategy against Proliferation of Weapons of Mass Destruction (OJ L 331, 17.12.2005, p. 34).

([3]) Council Joint Action 2007/185/CFSP of 19 March 2007 on support for OPCW activities in the framework of the implementation of the EU Strategy against Proliferation of Weapons of Mass Destruction (OJ L 85, 27.3.2007, p. 10).

([4]) Council Decision 2009/569/CFSP of 27 July 2009 on support for OPCW activities in the framework of the implementation of the EU Strategy against Proliferation of Weapons of Mass Destruction (OJ L 197, 29.7.2009, p. 96).

([5]) Council Decision 2012/166/CFSP of 23 March 2012 in support of activities of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the framework of the implementation of the EU Strategy against Proliferation of Weapons of Mass Destruction (OJ L 87, 24.3.2012, p. 49).

([6]) Council Decision 2013/726/CFSP of 9 December 2013 in support of the UNSCR 2118 (2013) and OPCW Executive Council EC-M-33/Dec 1, in the framework of the implementation of the EU Strategy against Proliferation of Weapons of Mass Destruction (OJ L 329, 10.12.2013, p. 41).

([7]) Council Decision (CFSP) 2015/259 of 17 February 2015 in support of activities of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the framework of the implementation of the EU Strategy against Proliferation of Weapons of Mass Destruction (OJ L 43, 18.2.2015, p. 14).

([8]) Council Decision (CFSP) 2017/2302 of 12 December 2017 in support of the OPCW activities to assist clean-up operations at the former chemical weapons storage site in Libya in the framework of the implementation of the EU Strategy against Proliferation of Weapons of Mass Destruction (OJ L 329, 13.12.2017, p. 49).

([9]) Council Decision (CFSP) 2017/2303 of 12 December 2017 in support of the continued implementation of UN Security Council Resolution 2118 (2013) and OPCW Executive Council decision EC-M-33/DEC.1 on the destruction of Syrian chemical weapons, in the framework of the implementation of the EU Strategy against proliferation of weapons of mass destruction (OJ L 329, 13.12.2017, p. 55).

([10]) Council Decision (CFSP) 2019/538 of 1 April 2019 in support of activities of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the framework of the implementation of the EU Strategy against Proliferation of Weapons of Mass Destruction (OJ L 93, 2.4.2019, p. 3).

(4) The continuation of such intensive and targeted assistance from the Union to the OPCW is necessary in the context of the active implementation of Chapter III of the EU Strategy.

(5) There is a need for further Union support for the Cyber Security and Resilience and Information Assurance Programme of the OPCW, which aims to enhance the capacity of the OPCW to maintain appropriate levels of cyber security and resilience in addressing current and emerging challenges related to cyber security,

HAS ADOPTED THIS DECISION:

Article 1

1. For the purpose of giving immediate and practical application to certain elements of the EU Strategy, the Union shall support a project of the OPCW with the following objectives:

— upgrading ICT infrastructure in line with the OPCW's institutional business continuity framework, with a strong focus on resilience, and

— ensuring privileged access governance, as well as physical, logical and cryptographic information management and separation for all strategic and mission networks of the OPCW.

2. In the context of paragraph 1, the Union-supported activities of the project of the OPCW, which are in compliance with the measures set out in Chapter III of the EU Strategy, shall be the following:

— operationalisation of an enabling environment for ongoing cyber security and resilience efforts within multi-site OPCW operations,

— designing of customised solutions for on-premises and cloud-based system integration and configuration with OPCW ICT systems and privileged access management (PAM) solutions, and

— initiation and testing of PAM solutions.

3. A detailed description of the Union-supported activities of the OPCW referred to in paragraph 2 is set out in the Annex.

Article 2

1. The High Representative of the Union for Foreign Affairs and Security Policy ('the HR') shall be responsible for the implementation of this Decision.

2. Technical implementation of the project referred to in Article 1 shall be carried out by the OPCW Technical Secretariat ('the Technical Secretariat'). It shall perform that task under the responsibility and the control of the HR. For that purpose, the HR shall enter into the necessary arrangements with the Technical Secretariat.

Article 3

1. The financial reference amount for the implementation of the project referred to in Article 1 shall be EUR 2 151 823.

2. The expenditure financed by the amount set out in paragraph 1 shall be managed in accordance with the procedures and rules applicable to the general budget of the Union.

3. The Commission shall supervise the proper management of the expenditure referred to in paragraph 2. For that purpose, it shall conclude the necessary agreement with the Technical Secretariat. That agreement shall stipulate that the Technical Secretariat is to ensure visibility of the Union contribution, commensurate with its size, and specify measures to facilitate the development of synergies and to avoid the duplication of activities.

4. The Commission shall endeavour to conclude the agreement referred to in paragraph 3 as soon as possible after the entry into force of this Decision. It shall inform the Council of any difficulties in that process and of the date of conclusion of the agreement.

Article 4

The HR shall report to the Council on the implementation of this Decision on the basis of regular reports prepared by the Technical Secretariat. The HR reports shall form the basis for the evaluation carried out by the Council. The Commission shall provide information on the financial aspects of the project referred to in Article 1.

Article 5

1. This Decision shall enter into force on the date of its adoption.

2. This Decision shall expire 24 months after the date of conclusion of the agreement referred to in Article 3(3). However, it shall expire six months after its entry into force if that agreement has not been concluded by that time.

Done at Luxembourg, 21 June 2021.

For the Council
The President
J. BORRELL FONTELLES

ANNEX

PROJECT DOCUMENT

1. Background

The OPCW is required to maintain infrastructure that permits information sovereignty in a manner commensurate with privileged access classifications, appropriate handling routines and existing threats whilst remaining capable of defending against emerging risks. The OPCW continues to consistently face serious and emerging risks in relation to cyber-security and cyber-resilience. The OPCW is a target of highly skilled, resourced and motivated actors. These actors continue to attack the confidentiality and integrity of the OPCW's information and infrastructure assets on a frequent basis. To respond to the concerns that recent cyber-attacks, current political considerations, and COVID-19 crisis underlined, and taking into account the unique requirements posed by the nature of the work of the OPCW to deliver on the mandate of the CWC, it is clear that essential investment in technical capabilities is necessary.

Under the OPCW's Special Fund for CyberSecurity, Business Continuity, and Physical Infrastructure Security, the OPCW has designed its Cyber Security and Resilience and Information Assurance Programme (OPCW Programme) with 47 activities to address cyber security challenges that have been experienced in recent times. The OPCW Programme is aligned to best practice as promoted by entities such as the European Union Agency for Cyber Security (ENISA) or using concepts related to the European Directive on Security of Network and Information Systems (NIS) pertaining to Telecoms and Defence. Collectively the OPCW Programme covers the following thematic areas: classified and unclassified networks; policy and governance; detection and response; operations and maintenance; and telecommunications. Fundamentally the OPCW Programme is designed to enable OPCW to reduce opportunities for well-resourced and/or state-sponsored attackers to achieve their aims, and to mitigate risks from both external and insider threats from both a human and technical perspective. The Union support is structured as a Project of three activities that corresponds to two of the 47 OPCW Programme's activities.

2. Project Purpose

The overall purpose of the Project is to ensure that the OPCW Secretariat has the capacity to maintain appropriate level of cyber security and resilience in addressing recurrent and emerging cyber-security defence challenges at OPCW headquarters and auxiliary facilities, to enable delivery of OPCW's mandate and effective implementation of the CWC.

3. Objectives

— Upgrading ICT infrastructure in line with OPCW's institutional business continuity framework, with a strong focus on resilience;

— Ensuring privileged access governance, as well as physical, logical and cryptographic information management and separation for all strategic and mission networks.

4. Results

Expected results the Project contributes to are as follows:

— ICT equipment and services deliver robust system reliability (hybrid/geographical redundancy) and facilitate increased availability of ICT systems and services in support of business continuity;

— Minimization of abilities for any single factor or person to adversely impact confidentiality and integrity of information or systems within the OPCW.

5. Activities

5.1. Activity 1 – Operationalisation of an enabling environment for on-going cyber security and resilience efforts within multi-site OPCW operations

This activity seeks to ensure an enabling environment for smooth roll out of OPCW business continuity planning as related to cyber security and resilience. This will be achieved through addressing infrastructure upgrades – re-architecture and/or archival for OPCW business continuity across multi-site operations. As well as further facilitating and enabling the integration of privileged access governance into the business continuity planning and response processes.

5.2. Activity 2 – Designing of customized solution for on premise and cloud based systems integration and configuration with OPCW ICT systems and Privileged Access Management (PAM) solutions

This activity focuses on translating the enabling environment into a customized design for on premise and cloud based systems integration and configuration with OPCW ICT systems and PAM solutions. This is expected to increase the efficiency of ICT systems infrastructure and lead to the design of an integrated PAM system for critical assets that can deter, detect, and is in line with commensurate threat hunting capabilities.

5.3. Activity 3 – Initiation and testing of PAM solutions

This activity builds upon the infrastructure implemented and the PAM solutions designed to take integration and configuration from theory towards practice. Systems have to be mapped, profiled, and embedded into existing systems while taking associated policy and human factors into consideration. After which thorough testing verifies and assures the robustness of the system (all new systems have strong authentication for users and devices, appropriate information classification and protection, and advanced data loss prevention) in implementation and over time, will enable the OPCW Secretariat to identify and address gaps to the extent possible.

6. Duration

The total estimated duration of implementation funded through this project are expected to be incurred and concluded over a 24-month period.

7. Beneficiaries

Beneficiaries from the project will be OPCW Technical Secretariat personnel, policy-making organs, subsidiary bodies and CWC stakeholders including States Parties.

8. EU Visibility

The OPCW shall take all appropriate measures, within reasonable security considerations, to publicise the fact that this project has been funded by the Union.