EUROPEAN
COMMISSION

Brussels, 12.6.2026
COM(2026) 280 final

2026/0145 (NLE)

Proposal for a

COUNCIL IMPLEMENTING DECISION

authorising support from the EU Cybersecurity Reserve for Moldova and repealing Implementing Decision (EU) 2025/1458

(Text with EEA relevance)

2026/0145 (NLE)

Proposal for a

COUNCIL IMPLEMENTING DECISION

authorising support from the EU Cybersecurity Reserve for Moldova and repealing Implementing Decision (EU) 2025/1458

(Text with EEA relevance)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)[1], and in particular Article 19(4) thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) On 23 June 2022, the European Council granted Moldova the status of candidate country. The decision was based on fulfilment by Moldova of the conditions specified in the Commission's opinion of June 2022 on Moldova's membership application. On 14 December 2023, the European Council decided to open accession negotiations with Moldova, following the recommendation issued by the Commission.

(2) In its conclusions of 15 December 2022, the European Council affirmed that the Union would continue to provide all relevant support to Moldova as it dealt with the multifaceted impact of Russia's war of aggression against Ukraine.

(3) Cybersecurity incidents continue to cause economic and societal impacts both across the Union and at global level. Cyber threats are evolving particularly rapidly in certain EU candidate countries where possible significant or large-scale incidents have the potential to disrupt and damage critical infrastructure, interfere with the proper functioning of the economy and institutions or pose serious public security and safety risks for entities and citizens. This is particularly the case in Moldova where Russia conducts hybrid campaigns and cyber-attacks to threaten critical infrastructure, democratic processes and election infrastructure.

(4) Taking into account the unpredictable nature of cybersecurity attacks, the fact that they are often not confined to a specific geographical area and that they pose a high risk of spill-over, the strengthening of the resilience of neighbouring countries and their capacity to respond effectively to significant and large-scale cybersecurity incidents contributes to the protection of the Union, in particular the internal market and

[1] OJ L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj.

industry, as a whole. Therefore, Regulation (EU) 2025/38 provides that third countries that are party to an association agreement with the Union allowing for their participation in the Digital Europe Programme (the 'DEP') ('DEP-associated third countries') may be supported from the EU Cybersecurity Reserve (the 'Reserve'), in all or part of their territories, where this is provided for in the agreement associating the third country to DEP.

(5) In accordance with Article 19 of Regulation (EU) 2025/38, DEP-associated third countries are able to request support from the Reserve when the entities targeted and for which they request such support are entities operating in sectors of high criticality or other critical sectors and when the incidents detected lead to significant operational disruptions or might have spillover effects in the Union. A third country is only eligible for such support where that is specifically provided for in the agreement associating that country to the DEP. In addition, such third countries should remain eligible only while three criteria set out in Article 19(3) of Regulation (EU) 2025/38 are fulfilled. First, the third country is to comply in full with relevant terms of that agreement. Second, given the complementary nature of the Reserve, the third country is to have taken adequate steps to prepare for significant or large-scale equivalent cybersecurity incidents. Third, the provision of support from the Reserve is to be consistent with the Union's policy towards, and overall relations with, that country and with other Union policies in the field of security.

(6) The provision of support to DEP-associated third countries may affect relations with third countries and the Union's security policy, including in the context of the common foreign and security policy and the common defence and security policy. The Council acts on the basis of a Commission proposal, taking due account of the Commission's assessment of the three criteria referred to in Article 19(3) of Regulation (EU) 2025/38.

(7) Moldova has been heavily impacted by Russia's war of aggression against Ukraine, while being directly targeted by Russia's hybrid activities seeking to destabilise the country and undermine its path to Union accession. Against this backdrop, the Union has provided comprehensive support to Moldova in addressing the challenges it faces as a consequence of Russia's war of aggression against Ukraine, and to strengthen the country's resilience, security and stability in the face of direct destabilising activities by Russia.

(8) On 24 April 2023, the Council adopted Decision (CFSP) 2023/855 establishing a civilian European Union Partnership Mission in Moldova under the common security and defence policy in order to provide strategic advice and operational support in the areas of crisis management and hybrid threats. Since 2021, the Union has also provided consistent support though the European Peace Facility to strengthen Moldova's capacities in the military and defence area. The signing of the EU-Moldova Security and Defence Partnership on 21 May 2024 streamlined the structure of Union's cooperation with Moldova in key areas of peace, security, and defence. Furthermore, the Moldova Growth Plan, adopted by the Commission on 10 October 2024, aims to support Moldova's socioeconomic reforms and enhance its access to the internal market, with specific reforms expected in the area of cybersecurity governance.

(9) As Moldova had fulfilled the criteria set out in Article 19(3) of Regulation (EU) 2025/38, support from the Reserve for Moldova was authorised by Council

Implementing Decision (EU) 2025/1458[2] on 14 July 2025. Since then, Moldova has been eligible to benefit from support in responding to cybersecurity incidents.

(10) In accordance with Article 19(4) of Regulation 2025/38, Implementing Decision (EU) 2025/1458 is to apply for a maximum of one year and may be renewed. The Commission has reassessed the three criteria set out in Article 19(3) of Regulation (EU) 2025/38 and considers them fulfilled. It has also consulted the High Representative of the Union for Foreign Affairs and Security Policy when conducting this assessment.

(11) As the agreement associating Moldova to the Digital Europe Programme provides for support from the Reserve and as that country fulfils the criteria set out in Article 19(3) of Regulation (EU) 2025/38, support for Moldova from the Reserve should still be authorised. Implementing Decision (EU) 2025/1458 should therefore be renewed pursuant to Article 19(4) of Regulation 2025/38 and replaced by this Implementing Decision.

(12) Implementing Decision (EU) 2025/1458 should be repealed,

HAS ADOPTED THIS DECISION:

Article 1

The provision of support from the EU Cybersecurity Reserve to the Republic of Moldova within the meaning of Article 19 of Regulation (EU) 2025/38 is hereby authorised.

Article 2

Implementing Decision (EU) 2025/1458 is repealed.

This Decision shall enter into force on 15 July 2026 and shall apply for one year.

Done at Brussels,

For the Council
The President

[2] OJ L, 2025/1458, 18.7.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1458/oj.