4 June 2024

Memorandum of Understanding on cooperation between the European Banking Authority, the European Insurance and Occupational Pensions Authority, the European Securities and Markets Authority, and the European Union Agency for Cybersecurity

Having regard to Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA)[1]; and

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)[2];

The European Supervisory Authorities (ESAs), including the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), the European Securities and Markets Authority (ESMA), and the European Union Agency for Cybersecurity (ENISA) and which collectively are known as the parties;

HAVE REACHED THE FOLLOWING UNDERSTANDING:

Article 1
Purpose

The purpose of this Memorandum of Understanding (MoU) is to set out the framework for cooperation and exchange of information between the ESAs and ENISA in the areas covered by the NIS2 Directive, DORA and other areas of mutual interest.

[1] OJ L 333, 27.12.2022, p. 1.
[2] OJ L 333, 27.12.2022, p. 164.

Article 2
Strategic cooperation

(1) The parties will cooperate to implement the tasks of common interest stemming from the NIS2 Directive and DORA, in particular the reporting of major ICT-related incidents, the development of draft technical standards, the establishment of mechanisms to share effective practices across sectors, or the provision of technical advice and sharing of hands-on experience on oversight activities.

(2) ENISA will facilitate the participation and active engagement of the ESAs in the activities of the NIS Cooperation Group, where relevant.

(3) The ESAs will facilitate the participation and active engagement of ENISA in the Oversight Forum and where necessary, the Joint Oversight Network.

(4) The parties will collaborate on the implementation of efficient incident reporting processes for the EU financial sector in line with the NIS2 Directive and DORA incident reporting implementing acts.

(5) ENISA will support the ESAs in the implementation of an IT tool for incident reporting purposes based on ENISA's Cyber Incident, Reporting and Analysis System tool (CIRAS).

(6) The parties will collaborate on the development of the pan-European systemic cyber incident coordination framework (EU-SCICF)[3].

(7) The parties will collaborate and coordinate on cybersecurity aspects and strengthen capabilities, knowledge, and skills in areas of mutual interest.

(8) The parties will exchange information and views while preparing the work plan and other documents that are relevant to the areas of cooperation identified in this MoU.

(9) The parties will exchange information on upcoming activities on emerging technologies of mutual concern and exchange views on forthcoming opinions and guidance of common strategic interest, as deemed relevant by the parties.

(10) The parties will invite each other to relevant expert meetings and collaborate in research and other related activities where appropriate.

Article 3

[3] Recommendation of the European Systemic Risk Board of 2 December 2021 on a pan-European systemic cyber incident coordination framework for relevant authorities (ESRB/2021/17), OJ C 134, 25.3.22, p.1.

Single Contact Point

(1) The parties will establish a Single Contact Point (SCP), composed of staff members of the parties, appointed by the parties as identified in the Annex to this MoU.

(2) The SCP will be responsible for coordinating the parties' cooperation and regular updates to this MoU and the work plan.

(3) The SCP will meet at least once a year to:

a. discuss and review matters related to the work plan further set out in Article 4,

b. identify further areas of cooperation, and

c. exchange views on main current and future challenges for cybersecurity, including analyses of emerging technologies and threats.

Article 4
Work plan

(1) The SCP will aim to agree on a work plan at least once a year, on the basis of the annual and multi-annual work programmes of each of the parties.

(2) This plan will specify the initiatives and actions (e.g. workshops, trainings and discussion forums) and include the distribution of tasks between the parties for the implementation of this MoU.

Article 5
Confidentiality

(1) The parties may not disclose confidential information exchanged in the framework of this MoU to third parties without the prior written consent of the originating party. This does not prevent the parties from sharing information in accordance with DORA, the NIS2 Directive and any other applicable Union legal act.

(2) The parties are bound by the professional secrecy regime established in their respective legal frameworks.

(3) The parties may share with one another insights and data, with the purpose of:

a. enhancing oversight and coordination,

b. responding to cyber threats and operational disruptions, and

c. strengthening the overall resilience of the digital ecosystem in the EU.

(4) Any confidential information exchanged by the parties under this MoU will be used only to the extent and level of detail necessary to the exercise by the parties of their respective tasks and duties attributed under the applicable Union legal acts.

Article 6
Implementation, duration and revision

(1) This MoU sets forth a statement of intent and does not create any directly or indirectly enforceable rights or legally binding obligations for the parties or any third party. The parties will use their best efforts to reach an amicable solution for any disagreement relating to the interpretation or application of this MoU.

(2) The parties may agree to establish joint or bilateral service level agreements (SLAs) on incident reporting, cybersecurity audits, trainings or other topics within their fields of competence.

(3) This MoU will come into effect on the day following the date of its signature by all parties (the last signing Party).

(4) This MoU is valid for three years and will automatically renew for additional three-year periods unless a party provides prior written notice of termination, at least two weeks before the date of the automatic renewal.

(5) Amendments to this MoU can be done by a mutual agreement at any time, except for amendments to the Annex which will be notified by the amending party to the other parties. Any such amendments, supplements or terminations will be in writing.

Signatures

For the European Banking Authority (EBA),

José Manuel Campa, Chairperson

[SIGNED]

For the European Insurance and Occupational Pensions Authority (EIOPA),

Petra Hielkema, Chairperson

[SIGNED]

For the European Securities and Markets Authority (ESMA),

Verena Ross, Chair

[SIGNED]

For the European Union Agency for Cybersecurity (ENISA),

Juhan Lepassaar, Executive Director

[SIGNED]

Annex
Members – Single Contact Point

EBA	Rūta Merkevičiūtė Head of Unit Digital Finance Ruta.Merkeviciute@eba.europa.eu
EIOPA	Ana Teresa Moutinho Head of Department Oversight AnaTeresa.Moutinho@eiopa.europa.eu
ENISA	Evangelos Ouzounis Head of Unit Policy development and implementation Evangelos.Ouzounis@enisa.europa.eu
ESMA	Alexandru Dincov Deputy Head of Department Data Intelligence and Technology (DIT) alexandru.dincov@esma.europa.eu