Organisation for Economic Co-operation and Development

DSTI/DPC/DS(2024)1/FINAL

Unclassified

English - Or. English

15 May 2024

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
DIGITAL POLICY COMMITTEE

Working Party on Digital Security

Conclusion of the Fifth Review of the 1997 Recommendation concerning Guidelines on Cryptography Policy

JT03543727

1. The OECD Recommendation concerning Guidelines for Cryptography Policy ("the Recommendation") [OECD/LEGAL/0289] was adopted by the OECD Council in 1997 to provide an international standard on how to promote the use of cryptography to foster confidence in the global digital environment without unduly jeopardising public safety, law enforcement and national security. The Guidelines for Cryptography Policy set out in the Annex to the Recommendation include a set of high-level policy principles to this effect.

2. In the Recommendation, the OECD Council recommended that Members review the Guidelines at least every five years with a view to improving international co-operation on issues relating to cryptography policy. The Digital Policy Committee (DPC)[1] carried out such reviews in 2002, 2007, 2012 and 2017, concluding that the Recommendation was adequate to address the issues and purpose for which it was formulated and that there was no need to revise it.

3. The Working Party on Digital Security (WPDS)[2] discussed the process for the review of the Recommendation's relevance at its 7th meeting in March 2023. On that basis, the Secretariat developed a background report to support the review of the Recommendation by providing up-to-date information about developments related to cryptography since 1997.

4. The background report was discussed at the Working Party's 8th meeting in November 2023. It includes an introduction to cryptography for policy makers and a presentation of the key technological trends potentially affecting cryptography in the future, namely homomorphic cryptography and quantum information technologies because they were identified as deserving further investigation in the conclusion of the fourth review of the Recommendation. The background report also covers technical and other responses to the challenge faced by law enforcement, such as "lawful hacking", key escrow and client-side scanning. A revised version of the background report was approved and declassified by the DPC at its 93rd session on 4-5 April 2024.

5. Also at its 8th meeting, the WPDS discussed the next steps for the Recommendation based on these elements, including the possibility of developing and issuing a questionnaire to delegates about the Recommendation's continued relevance. They agreed that the Secretariat would make a proposal as to the next steps of the review based both on the meeting discussions and written comments that the Secretariat would receive from delegates during the usual three-week period following the meeting.

6. The feedback indicated agreement that there was no need to implement a survey. The feedback also consistently supported the conclusion that the Recommendation continued to be adequate to address the issues and purpose for which it was developed, and that there was no need to revise it at this stage. More specifically, some delegations pointed out that technologies such as quantum information technologies and fully homomorphic encryption, presented in the background report, might have an impact on the Recommendation's relevance when they are more mature. However, these delegations concluded that it would be premature at this stage to find that such technologies had altered the relevance of the Recommendation.

7. Moving forward, when it adopted the latest set of OECD Digital Security Recommendations in 2022, the Council "noted that it will receive a joint report on the implementation, dissemination and continued relevance of all digital security-related Recommendations in five years' time" (i.e. in 2027). Accordingly, the present document will be the last report dedicated solely to the Recommendation concerning Guidelines for Cryptography Policy, as the next review will be carried out jointly with the other OECD Digital Security Recommendations.

[1] Previously called the Committee on Digital Economy Policy (CDEP), and the Committee for Information, Computer and Communications Policy (ICCP) prior to that.

[2] Previously called the Working Party on Security in the Digital Economy (WPSDE).

8. Considering the above, the WPDS proposed to the DPC to conclude that the Recommendation continues to be adequate to address the issues and purpose for which it was developed and that it does not need to be revised at this stage. The DPC agreed with this proposal at its 93rd session on 4-5 April 2024.