



NIS Cooperation Group

About the NIS Cooperation Group

The Group's overall mission is to achieve a high common level of security for network and information systems in the European Union. It supports and facilitates the strategic cooperation and the exchange of information among EU Member States. The NIS Cooperation Group's tasks are explicitly described in Article 11 of the [NIS Directive](https://digital-strategy.ec.europa.eu/en/policies/nis-directive) (<https://digital-strategy.ec.europa.eu/en/policies/nis-directive>).

The NIS Cooperation Group functions according to the [European Commission Implementing Decision of 1 February 2017](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32017D0179&from=EN) (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32017D0179&from=EN>) and follows its own [rules of procedure \(.pdf\)](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51975) (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51975). The European Commission serves as the secretariat of the Group. The Cooperation Group meets regularly. The European Commission publishes the [agendas of all NIS Cooperation meetings](https://digital-strategy.ec.europa.eu/en/library/nis-cooperation-group-meetings-agendas) (<https://digital-strategy.ec.europa.eu/en/library/nis-cooperation-group-meetings-agendas>).

On the operational side, the NIS Cooperation Group is supported by the work of the network of Computer Security Incident Response Teams (CSIRTs), dedicated to sharing information about risks and ongoing threats, and cooperating on specific cybersecurity incidents. The CSIRTs network was established under Article 12 of the NIS Directive, which also defines its role. The NIS Cooperation Group provides strategic guidance for the activities of the CSIRTs network.

The NIS Cooperation Group is also working closely with the [European Cooperation Network on Elections](https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en) (https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en) to counter threats to electoral processes under a new joint operational mechanism set-up as a part of the [European Democracy Action plan](https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en) (https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en).

Members

The NIS Cooperation Group is composed of representatives of the EU Member States, the European Commission and the [EU Agency for cybersecurity \(ENISA\)](http://www.enisa.europa.eu/) (<http://www.enisa.europa.eu/>). The Chairmanship in position is filled by the Member State holding the [Presidency of the Council of the European Union \(EU\)](http://www.consilium.europa.eu/en/council-eu/presidency-council-eu/) (<http://www.consilium.europa.eu/en/council-eu/presidency-council-eu/>).

Every EU Member State has designated a [single point of contact \(.pdf\)](https://ec.europa.eu/newsroom/dae/redirection/document/97902) (<https://ec.europa.eu/newsroom/dae/redirection/document/97902>) on the security of network and information systems that is responsible for ensuring cross-border cooperation with other Member States and with the Cooperation Group.

Publications

Among the key outputs of the NIS Cooperation Group, there are non-binding guidelines to the EU Member States to allow effective and coherent implementation of the NIS Directive across the EU and to address wider cybersecurity policy issues.

Since its establishment, the Group has published the following documents:

General reports

- [Technical Guideline: Security Measures for Top-Level-Domain Name Registries \(.pdf\)](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=84325) (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=84325)
- [Reference document on security measures for Operators of Essential Services \(.pdf\)](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643) (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643)
- [Reference document on incident notification for Operators of Essential Services \(circumstances of notification\) \(.pdf\)](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53644) (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53644)
- [Compendium on cyber security of election technology \(.pdf\)](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53645) (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53645)
- [Cybersecurity incident taxonomy \(.pdf\)](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53646) (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53646)
- [Guidelines on notification of Operators of Essential Services incidents \(formats and procedures\) \(.pdf\)](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53677) (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53677)
- [Guidelines on notification of Digital Service Providers incidents \(formats and procedures\) \(.pdf\)](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53677) (https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53677)

- https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53675
- [Reference document on the identification of Operators of Essential Services \(modalities of the consultation process in cases with cross-border impact\) \(.pdf\) \(https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53661\)](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53661)
- [Guidelines for the Member States on voluntary information exchange on cross-border dependencies \(.pdf\) \(https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=65182\)](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=65182)
- [Sectorial implementation of the NIS Directive in the Energy sector \(.pdf\) \(https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62799\)](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62799)
- [Synergies in Cybersecurity Incident Reporting \(.pdf\) \(https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72147\)](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72147)
- [Threats and risk management in the health sector under the NIS Directive \(.pdf\) \(https://ec.europa.eu/newsroom/ECCC/redirection/document/97124\)](https://ec.europa.eu/newsroom/ECCC/redirection/document/97124)
- [Guidelines on implementing national Coordinated Vulnerability Disclosure \(CVD\) policies \(https://ec.europa.eu/newsroom/dae/redirection/document/99973\)](https://ec.europa.eu/newsroom/dae/redirection/document/99973)
- [Compendium on Elections Cybersecurity and Resilience \(2024 Updated Version\) \(https://ec.europa.eu/newsroom/dae/redirection/document/103148\)](https://ec.europa.eu/newsroom/dae/redirection/document/103148)
- [EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors \(.pdf\) \(https://ec.europa.eu/newsroom/dae/redirection/document/107357\)](https://ec.europa.eu/newsroom/dae/redirection/document/107357)
- [Recommendations for the implementation of NIS2 Directive Article 28 \(Database of domain name registration data\) \(.pdf\) \(https://ec.europa.eu/newsroom/dae/redirection/document/108437\)](https://ec.europa.eu/newsroom/dae/redirection/document/108437)

Annual summary incident reports

- [Annual Report NIS Directive Incidents 2019 \(.pdf\) \(https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72146\)](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72146)
- [Annual Report NIS Directive Incidents 2020 \(.pdf\) \(https://ec.europa.eu/newsroom/dae/redirection/document/105731\)](https://ec.europa.eu/newsroom/dae/redirection/document/105731)
- [Annual Report NIS Directive Incidents 2021 \(.pdf\) \(https://ec.europa.eu/newsroom/dae/redirection/document/105729\)](https://ec.europa.eu/newsroom/dae/redirection/document/105729)
- [Annual Report NIS Directive Incidents 2022 \(.pdf\) \(https://ec.europa.eu/newsroom/dae/redirection/document/105730\)](https://ec.europa.eu/newsroom/dae/redirection/document/105730)
- [Annual Report NIS Directive Incidents 2023 \(.pdf\) \(https://ec.europa.eu/newsroom/dae/redirection/document/111612\)](https://ec.europa.eu/newsroom/dae/redirection/document/111612)

Cybersecurity of 5G networks

- a [risk assessment of 5G networks \(.pdf\) \(https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132\)](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132),
- a [toolbox of risk mitigating measures \(.pdf\) \(https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468\)](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468) for 5G networks
- Reports on the on Member States' progress in implementing the toolbox: [1st report \(.pdf\) \(https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68510\)](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68510); [2nd report \(.pdf\) \(https://ec.europa.eu/newsroom/dae/redirection/document/96519\)](https://ec.europa.eu/newsroom/dae/redirection/document/96519)
- a report on the [cybersecurity of Open RAN \(https://digital-strategy.ec.europa.eu/en/library/report-cybersecurity-open-ran\)](https://digital-strategy.ec.europa.eu/en/library/report-cybersecurity-open-ran)
- a report on the [cybersecurity and resiliency of the EU communications infrastructures and networks \(https://digital-strategy.ec.europa.eu/en/library/report-cybersecurity-and-resiliency-eu-communications-infrastructure-and-networks\)](https://digital-strategy.ec.europa.eu/en/library/report-cybersecurity-and-resiliency-eu-communications-infrastructure-and-networks)

Source URL: <https://digital-strategy.ec.europa.eu/policies/nis-cooperation-group>

© European Union, 2025 - [Shaping Europe's digital future \(https://digital-strategy.ec.europa.eu/en\)](https://digital-strategy.ec.europa.eu/en) - PDF generated on 29/03/2025

Reuse of this document is allowed, provided appropriate credit is given and any changes are indicated (Creative Commons Attribution 4.0 International license).

For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.