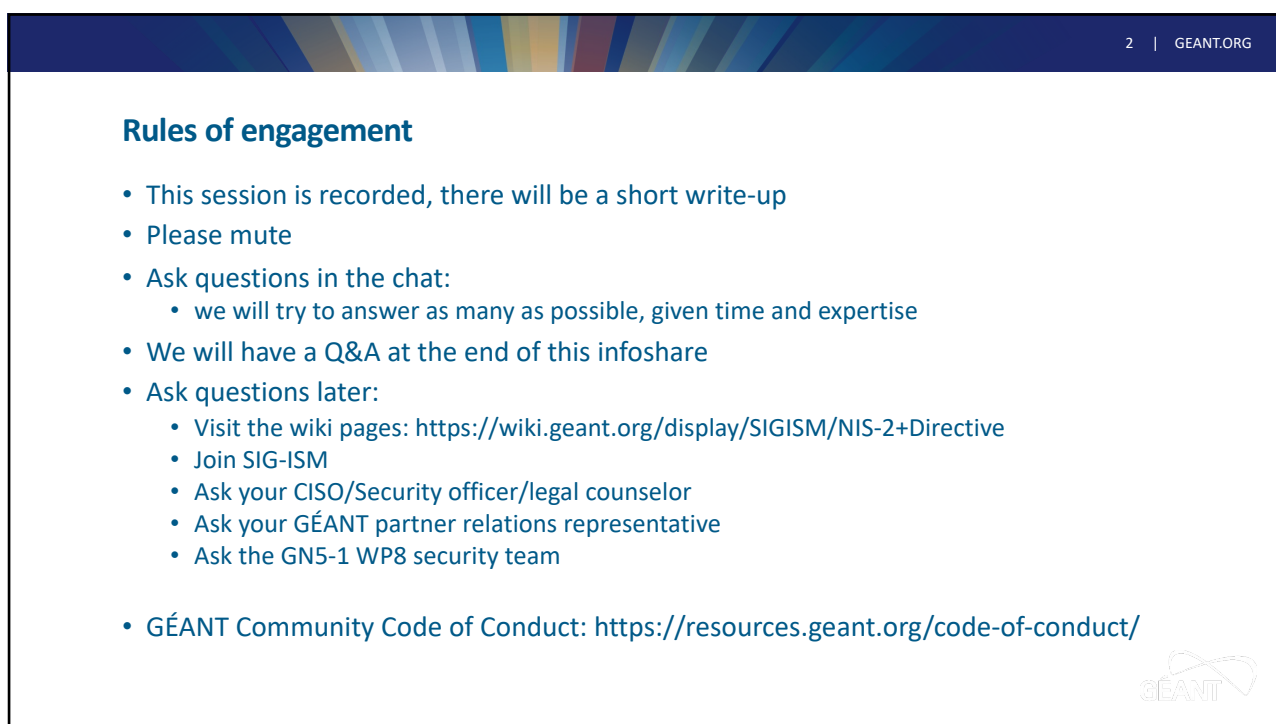
  
**EU Security Union – 6th INFOSHARE**  
NIS-2: State of affairs and next steps

Online Infoshare  
18 March 2024  
Public


1



2 | GEANT.ORG

### Rules of engagement

- This session is recorded, there will be a short write-up
- Please mute
- Ask questions in the chat:
  - we will try to answer as many as possible, given time and expertise
- We will have a Q&A at the end of this infoshare
- Ask questions later:
  - Visit the wiki pages: <https://wiki.geant.org/display/SIGISM/NIS-2+Directive>
  - Join SIG-ISM
  - Ask your CISO/Security officer/legal counselor
  - Ask your GÉANT partner relations representative
  - Ask the GN5-1 WP8 security team
- GÉANT Community Code of Conduct: <https://resources.geant.org/code-of-conduct/>



2

## Agenda

|       |   |                  |
|-------|---|------------------|
| 14.00 | Welcome and introduction                  | Alf Moens        |
| 14.10 | Questions, questions, questions           | Zoë Fischer      |
| 14.25 | Let's hear from you – information sharing | All participants |
| 15.00 | Closure                                   |                  |



3

## Quick Summary

- **NIS-2 directive** has been published on 15th of December 2022, and will be in action within 21 months from the "entry in force":
- **4th of October 2024:** (January 4th 2023+ 21 months) latest, but with the Council Recommendation **to do it ASAP.**
- Standards are still 'negotiated' via comitology (delegated Act)
  - Expect „Rulings” or „guidance” from ENISA and NIS Cooperation Group
- Obligations are „logical”, no real surprises



4

5 | GEANT.ORG

## The EU Security Union is complex and overlaps with the EU Digital priorities

The diagram illustrates the overlap between the EU Security Union and digital priorities. The Security Union is centered on 'The EU Security Strategy', which includes 'Tackling evolving threats' and 'A strong security ecosystem'. Digital priorities are represented by a cloud of interconnected circles, including acts like NIS2, CER, CRA, AI Act, and strategies like Digital Strategy, Data Strategy, and Industrial Policy. A legend on the right categorizes these into Infrastructure, Rights, and Funding.

European Commission, Factsheet: The EU 'Union Strategy' (9<sup>th</sup> of December 2020)

5

6 | GEANT.ORG

## Timelines for NIS2, CER, CRA

The timeline shows the legislative and enforcement paths for NIS2, CER, and CRA. NIS2 and CER follow a path from European legislation in 2022 to enforcement in 2025. CRA follows a similar path but with enforcement starting in 2024. A red box highlights that MSs have agreed to frontload enforcement for CRA before the legislation is transposed.

Due to the current alarm levels MS-s have agreed to frontload enforcement even before the legislation is transposed Critical infrastructure protection in digital sector modelled on 5G Cybersecurity Toolbox

6

8 | GEANT.ORG

### What is the NIS-2 directive about?

73 pages  
144 preambles  
64 Articles  
2 Annexes

A central blue oval labeled "Obligations for Essential and Important entities" is connected to seven surrounding blue ovals: "Obligations for Member States", "Implementation guidance, governance and control for MS", "Obligations to report security incidents", "International Collaboration", "Cybersecurity information sharing", "Vulnerability disclosure & European Vuln. database", and "Use of European cybersecurity certification schemes". A separate oval at the bottom is labeled "Union level coordinated security risk assessments of critical supply chains".

8

9 | GEANT.ORG

### Supervision and Sanctions

A central blue oval labeled "suspend temporarily a certification" is connected to four surrounding blue ovals: "Essential entities: ex ante / Important entities: ex post", "Periodic scans, audits, inspections by supervising body or 3rd parties", "administrative fines (maximum of at least EUR 7M or of a maximum of at least 1,4 % of the total worldwide annual turnover)", and "request that the relevant bodies, courts or tribunals, prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level in the essential entity from exercising managerial functions in that entity (essential enteties only)".

9

## What is the impact of NIS-2 for your organisation?

- It will depend!
- .tld, Internet exchange and DNS resolver are in scope
- Closed network services are not!
- Position Paper on Impact NIS-2 from NRENs in different positions
- Delays expected
- Self service
- Multiple supervisors
- ENISA: clarification on "multinational" situations

## The 'NEVERS' report

### Shaping Europe's digital future

[Home](#) | [Policies](#) | [Activities](#) | [News](#) | [Library](#) | [Funding](#) | [Calendar](#) | [Consultations](#) | [AI Office](#)

[Home](#) > [Library](#) > Report on the cybersecurity and resiliency of the EU communications infrastructures and networks

REPORT / STUDY | Publication 21 February 2024

### Report on the cybersecurity and resiliency of the EU communications infrastructures and networks

EU Member States, with the support of the European Commission and ENISA, the EU Agency for Cybersecurity, published a report on the cybersecurity and resiliency of Europe's communications infrastructures and networks. This marked another major step in the coordinated work at EU level on the security of telecommunications, and complements the work already done on 5G cybersecurity.

As a follow-up to the Nevers Call of 9 March 2022 and building on the coordinated work already done at EU-level to strengthen the security of 5G networks, Member States conducted a risk assessment on Europe's communications infrastructures and networks.

This risk assessment identified a number of threats for communication networks and infrastructure, such as wipers, ransomware attacks, supply chain attacks, physical attacks, sabotage, etc. These threats, taking advantage of vulnerabilities, could pose a significant risk for the security and resilience of the connectivity infrastructure. Based on these findings and in addition to the nine risk scenarios already identified in the EU Coordinated risk assessment on 5G networks, the report

#### Related topics

[Broadband](#) [Connectivity](#) [Cybersecurity](#)  
[Electronic communications and Privacy](#)  
[Telecom rules](#) [BEREC](#) [5G/6G](#)

12 | GEANT.ORG

**Any progress?**

**Let's hear from you**



12

13 | GEANT.ORG

**How can we help?**

GN5-1 WP8 T1: Best practices, guidelines and baselines

SIG-ISM wiki pages:  
<https://wiki.geant.org/display/SIGISM/NIS-2+Directive>



13

Questions?

Remarks?

### What you need to do NOW!

- Find out what your position is and try to have that confirmed
- Establish contacts in government
  
- Establish a baseline position
  - Use the GÉANT security baseline or any other checklist to verify your status on the main security subjects
  - Identify weak spots and gaps



16

17 | GEANT.ORG

## What to negotiate during transposition: NREN-s and GÉANT

- Scope
  - Domain
    - Public Administration
    - Education
  - Qualification of Specific entities
    - Essential: Digital infrastructures are here
    - Important
- National Cyber Security Strategy (examples)
  - Governance Framework
  - Public Procurement Specification
  - Policy on the open Internet and Submarine cables
  - Policy on support to R&D Communities

Suggestion

1. The opportunity to opt out is impossible
2. To be an important entity is not feasible ( as definition of RI is very specific)
3. Among Essential types Digital Infrastructure is the best. (avoid CER additional requirements)

Conclusion

Member States will differ, coordination among NREN/s is recommended

Objective

Minimize the burden and fragmentation

17



18 | GEANT.ORG

### Impact of NIS-2 for Research and Education: in scope or out-of-scope

Type of organisation

- Public Administration
- Registrar
- Internet exchange
- ...

Example of negotiations:

- Size\* of a tld determines whether registry is in/out scope
- However negotiations between Member States: NL 300.000+, D: 500+

Aim to be a digital infrastructure, either an essential or an important entity. Most NREN's should not be in scope of CER.

- Scoping decisions are made on a national (Member State) level

"The entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities" (art. 2.2.b)

"The entity is critical because of its specific importance at national ... level for the particular sector ..., or for other interdependent sectors" (art.2.2.e)

Essential or important?  
Same rules apply except the oversight

**\*Caution**  
The Size criteria is overruled by Article 2.2  
„Regardless of their size...“

18

19 | GEANT.ORG

### Article 21 Cybersecurity risk-management measures

“based on an all-hazards approach”

- a. Policies on risk analysis and information system security;
- b. incident handling;
- c. business continuity, such as backup management and disaster recovery, and crisis management;
- d. Supply chain security
- e. Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

- f. policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
- g. Basic cyber hygiene practices and training;
- h. Cryptography and, where appropriate, encryption;
- i. human resources security, access control policies and asset management;
- j. multi-factor authentication or continuous authentication solutions

RISK analysis → Security Measures

19

20 | GEANT.ORG

**SECTORS OF HIGH CRITICALITY (Annex I)**

- Energy
- Transport
- Banking
- Financial Market Infrastructure
- Health
- Drinking water
- Waste Water
- Digital infrastructure
- ICT Service management
- Public Administration
- Space

**Other Critical SECTORS (Annex II)**

- Postal and courier services
- Waste management
- Chemical industry and supply chain
- Food supply chain
- Manufacturing (limited)
- Digital providers
  - Online marketplace
  - Search engines
  - Social networking services platforms
- Research organisations

20

21 | GEANT.ORG

**SECTORS OF HIGH CRITICALITY (Annex I)**

- Energy
- Transport
- Banking
- Financial Market Infrastructure
- Health
- Drinking water
- Waste Water
- Digital infrastructure
- ICT Service management
- Public Administration
- Space

**Other Critical SECTORS (Annex II)**

- Postal and courier services
- Waste management

|                           |  |
|---------------------------|--|
| 8. Digital infrastructure | — Internet Exchange Point providers                                  |
|                           | — DNS service providers, excluding operators of root name servers    |
|                           | — TLD name registries  |
|                           | — Cloud computing service providers                                  |
|                           | — Data centre service providers                                      |
|                           | — Content delivery network providers                                 |
|                           | — Trust service providers  |
|                           | — Providers of public electronic communications networks             |
|                           | — Providers of publicly available electronic communications services |

- Research organisations

21

22

22 | GEANT.ORG

## What CSIRTs can do

### NIS 2 Directive: cybersecurity improvement for all

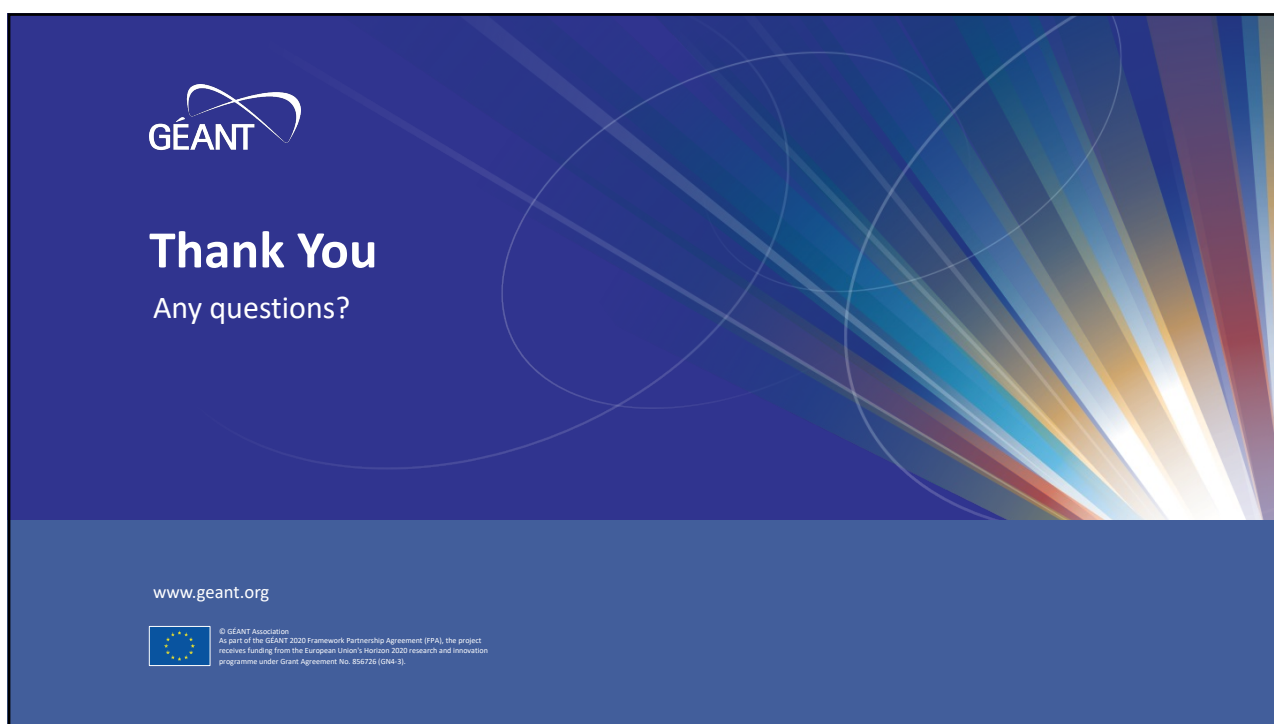
By [Andrew Cormack](#) 5 January 2023 No Comments

The final text of the revised [European Network and Information Security Directive \(NIS 2 Directive\)](#) has now been published. This doesn't formally apply in the UK, but does have some helpful comments on using data protection law to support network and information security. I've blogged about these previously but, since the final version significantly changes the draft numbering, I thought it was worth posting a revised index to those posts:

[CSIRT \(international\) Information Sharing](#): Draft Recital 69, which encouraged incident response and information sharing, is now split across Recitals 120 and 121. The former is now even more explicit that "entities should be encouraged and assisted by Member States to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhancing their capabilities to adequately prevent, detect, respond to or recover from incidents or to mitigate their

<https://regulatorydevelopments.iiscinvolve.org/wp/2023/01/05/nis-2-directive-cybersecurity-improvement-for-all/>

22




**GEANT**

# Thank You

Any questions?

[www.geant.org](http://www.geant.org)

 © GEANT Association  
As part of the GEANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856725 (GMA-3).

23