ECS600 Cybersecurity Compliance Seminar

Jonas Colmsjö

2025-04-14

University West

Question

A key requirement on EU member states in the Directive 2022/2555 (NIS2) is a National cybersecurity strategy (Article 7). Sweden released such a strategy, Nationell strategi för cybersäkerhet 2025-2029 (Skr 2024/25:121) on 20:th of March 2025. Evaluate to what extent the Swedish strategy meet the EU requirements.

NIS2 Implementation Status

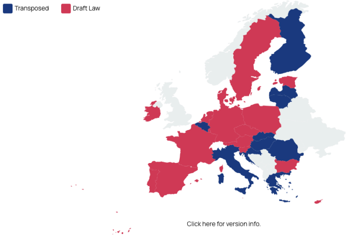
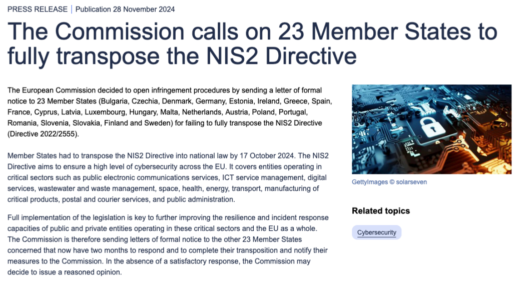


Figure 1: Status



PRESS RELEASE | Publication 28 November 2024

The Commission calls on 23 Member States to fully transpose the NIS2 Directive

The European Commission decided to open infringement procedures by sending a letter of formal notice to 23 Member States (Bulgaria, Czechia, Denmark, Germany, Estonia, Ireland, Greece, Spain, France, Cyprus, Latvia, Luxembourg, Hungary, Malta, Netherlands, Austria, Poland, Portugal, Romania, Slovenia, Slovakia, Finland and Sweden) for failing to fully transpose the NIS2 Directive (Directive 2022/2555).

Member States had to transpose the NIS2 Directive into national law by 17 October 2024. The NIS2 Directive aims to ensure a high level of cybersecurity across the EU. It covers entities operating in critical sectors such as public electronic communications services, ICT service management, digital services, wastewater and waste management, space, health, energy, transport, manufacturing of critical products, postal and courier services, and public administration.

Full implementation of the legislation is key to further improving the resilience and incident response capacities of public and private entities operating in these critical sectors and the EU as a whole. The Commission is therefore sending letters of formal notice to the other 23 Member States concerned that now have two months to respond and to complete their transposition and notify their measures to the Commission. In the absence of a satisfactory response, the Commission may decide to issue a reasoned opinion.

GettyImages © solarseven

Related topics

Cybersecurity

Figure 2: Lack of progress

Source: https://ecs-org.eu/activities/nis2-directive-transposition-tracker, Accessed 250414; https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive, Accessed 250414

NIS2 Article 7 National cybersecurity strategy (1/2)

1. Each Member State shall adopt a national cybersecurity strategy that provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include:

(a) **objectives and priorities** of the Member State's cybersecurity strategy covering in particular the sectors referred to in Annexes I and II;

(b) a **governance framework** to achieve the objectives and priorities referred to in point (a) of this paragraph, including the policies referred to in paragraph 2;

(c) a governance framework **clarifying the roles and responsibilities** of relevant stakeholders at national level, underpinning the cooperation and coordination at the national level between the competent authorities, the single points of contact, and the CSIRTs under this Directive, as well as coordination and cooperation between those bodies and competent authorities under sector-specific Union legal acts;

(d) a mechanism to **identify relevant assets** and an assessment of the risks in that Member State;

(e) an identification of the **measures ensuring preparedness for, responsiveness to and recovery from incidents**, including cooperation between the public and private sectors;

(f) a list of the various **authorities and stakeholders involved in the implementation** of the national cybersecurity strategy;

(g) a **policy framework** for enhanced coordination between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2557 for the purpose of information sharing on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks, as appropriate;

(h) a plan, including necessary measures, to **enhance the general level of cybersecurity awareness among citizens**.

These requirements have been evaluated.

NIS2 Article 7 National cybersecurity strategy (2/2)

2. As part of the national cybersecurity strategy, Member States shall in particular adopt policies:

(a) addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services;

(b) on the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including in relation to cybersecurity certification, encryption and the use of open-source cybersecurity products;

(c) managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure under Article 12(1);

(d) related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables;

(e) promoting the development and integration of relevant advanced technologies aiming to implement state-of-the-art cybersecurity risk-management measures;

(f) promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, stakeholders and entities;

(g) supporting academic and research institutions to develop, enhance and promote the deployment of cybersecurity tools and secure network infrastructure;

(h) including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities in accordance with Union law;

(i) strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope of this Directive, by providing easily accessible guidance and assistance for their specific needs;

(j) promoting active cyber protection.

*These requirements have **not** been evaluated in order to keep the scope manageable.*

Sweden's national strategy for cybersecurity (1/2)

The document "Nationall strategi för cybersäkerhet 2025-2029" is currently only available in Swedish.

It is to be submitted to EU (in English one would assume) on 20 June the latest (NIS2 Article 7 3§)

Sweden’s national strategy for cybersecurity (2/2)

Innehål

1. Vision
2. Den nationella cybersäkerhetsstrategins utgångspunkter
3. Cybersäkerhetslandskapet
4. Regeringens inriktning
   4.1 Pelare A: Systematiskt och effektivt cybersäkerhetsarbete
   4.2 Pelare B: Utvecklad kunskap och kompetens inom cybersäkerhet
   4.3 Pelare C: Förmåga att förhindra och hantera cybersäkerhetsincidenter
5. Genomförande och uppföljning
6. Översikt över utmaningar och mål
7. Begreppsförteckning
   Bilaga 1 Handlingsplan 2025
   Bilaga 2 Organisationer med roller och ansvarsområden inom cybersäkerhet

A first check

1. Vision
2. Den nationella cybersäkerhetsstrategins utgångspunkter
3. Cybersäkerhetslandskapet
4. Regeringens inriktning
   4.1 Pelare A: Systematiskt och effektivt cybersäkerhetsarbete
   4.2 Pelare B: Utvecklad kunskap och kompetens inom cybersäkerhet
   4.3 Pelare C: Förmåga att förhindra och hantera cybersäkerhetsincidenter
5. Genomförande och uppföljning
6. Översikt över utmaningar och mål
7. Begreppsförteckning
   Bilaga 1 Handlingsplan 2025
   Bilaga 2 Organisationer med roller och ansvarsområden inom cybersäkerhet

NIS 2 requirements:
a) objectives ✓ and priorities
b) governance framework
c) clarification of the roles and responsibilities
d) identification of relevant assets
e) risk-management measures
f) measures ensuring preparedness for, responsiveness to and recovery from incidents
f) authorities and stakeholders involved in the implementation ✓
g) policy framework
h) enhance the general level of cybersecurity awareness among citizens

The Swedish Cybersecurity strategy has little (or no) resemblance with the EU NIS2 Directive!

A note on roles and responsibilities (1/2)

The current Swedish framework has assigned the following Competent Authorities (Tillsynsmyndigheter):

- Statens Energimyndighet
- Finansinspektionen
- IVO
- Livsmedelsverket
- PTS
- Transportstyrelsen

A note on roles and responsibilities (2/2)

The Official Report, Nya regler om cybersäkernet, SOU 2024:18 (The Swedish Government Official Report New rules regarding cybersecurity) mention responsibilities.

The report mentoin that having multiple competent authorities has led to fragmentation and incoherent application of the NIS-directive.

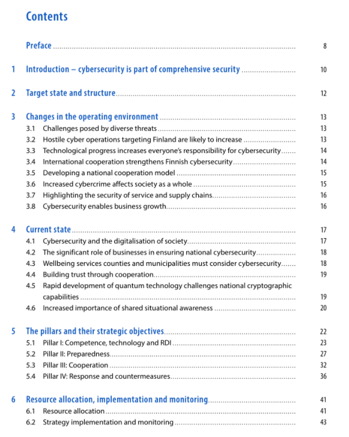
The report also notes that the current oversight is in insufficient. An example is a quote from a report from Riksrevisionen: "...Transportstyrelsen bedrivit mycket lite faktiskt tillsyn enligt NIS-refleringen", roughly translated: "...The transportation authority has performed very little oversight according to the NIS directive"

Still, the report suggest that the current framework for roles and responsibilities is used also going forward while noting that the number of parties that each authority is responsible for will be substantially larger.

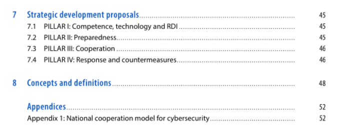
The real driver behind the Swedish Cybersecurity strategy?

If NIS2 isn't the real driver, then what is?

Example: **Finland's Cyber Security Strategy 2024–2035**



Contents



The headings of the Finnish strategy is very similar to the Swedish!

Also, the US Cybersecurity Strategy from 2023 has a similar structure.

Is perhaps NATO the driving force?

The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub

"The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organisation accredited in 2008 by NATO's North Atlantic Council as a 'Centre of Excellence'. Located in Tallinn, Estonia, the Centre is currently supported by Estonia, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, and the USA as Sponsoring Nations. The Centre is not part of NATO's command or force structure, nor is it funded by NATO. However, it is part of a wider framework supporting NATO Command Arrangements."

NATO CCD COE has extensive experience and has developed the National Cyber Security Strategy Framework Manual

Source: https://ccdcoe.org/library/publications/national-cyber-security-strategy-guidelines/

Summary

The Swedish National Strategy for Cybersecurity 2025-2030 meet few of the requirements set out in Directive 2022/2555 (NIS2)

The organisation of oversight from Swedish Competent Authorities is unclear and has been noted to be dysfunctional!

The Strategy does however resemble the Cybersecurity Strategies of other NATO members.

It is also noted in an Appendix that the Swedish Security Service (SÄPO) and The Swedish Armed Forces (Försvarsmakten) are responsible for operations deemed most import from a security perspective.

- This is in practice handled by the Swedish National Defence Radio Establishment (FRA)
- “FRA also provides cyber security services for selected government authorities and individual business operators who handle information deemed to be sensitive from a vulnerability point of view or in a security or defense policy aspect.” Source: https://www.fra.se/system/engelska/english.4.55af049f184e92956c42ca2.html

There is little public information regarding FRA:s work though

Thank You!