Our reference: 21-2124

Memorandum regarding PTS' positions on NIS 2 proposal

1. Introduction/Background

On the 16th of December 2020 the European Commission published a proposal for a NIS 2 Directive[1] (henceforth, NIS 2) intended to replace the current NIS Directive[2]. NIS 2 signifies broad changes and updates to the current NIS framework. While the Swedish Post and Telecom Authority (PTS) can see numerous benefits with the updated proposal, there are areas where PTS believes that the changes might create more issues than they solve. However, if these changes are to be included in the final proposal, certain parts of the NIS 2 framework need to be clarified and amended in order to create a comprehensive directive.

This memorandum contains the positions of PTS regarding necessary clarifications of NIS 2. Please note that this memorandum does not represent the positions of Sweden as a Member State, but solely the positions of PTS as a national regulatory authority according to the EECC[3] and as a supervisory body according to the NIS legal framework as well as the eIDAS Regulation.

2. Summary

In summary, the positions of PTS are as follows:

- Neither telecom nor trust services should be included in NIS 2 as new sectors. If they are included, certain areas of the proposal must be clarified and amended.
- The scope of NIS 2, regarding what parts of the designated services are regulated, must be clarified in NIS 2.

[1] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[3] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

Post- och telestyrelsen
Postadress: Box 5398, 102 49 Stockholm
Besöksadress: Valhallavägen 117 A
Telefon: 08-678 55 00
E-post: pts@pts.se
www.pts.se

- The distinction between electronic communications services and social networking services platforms must be clarified in NIS 2.
- Having certain entities be under the jurisdiction of the Member State where they have their main establishment (Article 24) could result in slow-moving supervision. Further, "decisions on risk management measures" could be taken locally or regionally, so this provision might not provide a clear enough guidance when considering the "main establishment" of an entity.

3. Positions

3.1. The scope of telecom and trust services vs the scope of NIS

PTS' primary position is that neither electronic communications services and networks (telecom services) nor trust services should be included as new sectors in the NIS Directive at this point, for reasons previously communicated[4] to the Commission. If these changes are included in the final proposal, the following needs to be addressed.

There is a lack of clarity regarding the scope of NIS 2. The inclusion of new sectors, previously regulated in legal frameworks with a different focus than NIS, raises questions concerning where to draw the line on what is and is not regulated. This is most notably relevant when it comes to telecom services as well as trust services.

The current scope of the EECC is not limited to a telecom provider's network and information systems. Rather, it is meant to encompass the electronic communication service (or network) as a whole. A SIM swap attack, for example, targeting a telecom provider's customer service, would most likely not give an attacker access to more than a single subscriber's subscription information – in other words: only the essential service itself (telecom), and not the network and information systems used in the operations.

Simply put, there seems to be a gap between the telecom services currently regulated in the EECC, and the network and information systems currently regulated in the NIS framework. The same can be said of trust services, which are currently regulated in its entirety in the eIDAS Regulation[5], compared to the much narrower NIS scope. To streamline the different frameworks, it is not sufficient to simply move the relevant articles from one legal text to

[4] See *Memorandum regarding PTS' preliminary positions on certain proposed changes to the NIS Directive*, 2020-11-12, reference: 20-12896, as well as *Memorandum regarding PTS' initial positions on trust services being included in the NIS 2 framework*, 2021-02-15, reference: 21-1326.

[5] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

another; further harmonisation and elaboration is needed to make sure that the scope remains the same.

During NIS 2 discussions in, for example, the ECASEC, BEREC and FESA meetings, questions around scope have been raised to the European Commission (the Commission). As PTS understands it, the explanation given by the Commission to ECASEC, BEREC and FESA concerning the scope is that both telecom services and trust services within the framework of NIS 2 will have the exact same scope as the EECC and the eIDAS Regulation respectively. However, Article 18 of NIS 2 specifies that the measures taken shall manage the risks posed to *the security of network and information systems which those entities use in the provision of their services*. If NIS 2 is intended to have the same scope as the EECC and the eIDAS Regulation regarding the security of telecom services and trust services, it must be substantially clarified in the NIS 2 Directive. This could possibly be achieved by, for example, drafting additional articles conveying exceptions to the rule focusing on network and information systems.

Lastly, thought should be given as to whether the services in the Digital Infrastructure sector will have a broader scope than the services in other NIS sectors. Will, for example, the essential service of water distribution be regulated in its entirety in NIS 2, or will only the network and information systems which distributors use in the provision of that service be regulated? The commentary from the Commission regarding the scope of telecom and trust services implies that there will be a difference in scope. This must be analysed and clarified.

3.2. Clearer distinctions

Adjacent to the above point regarding clarification on the scope, additional clarity is needed on certain definitions and distinctions.

Telecom services and their subcategories

According to NIS 2, providers are divided up into Essential Entities (EE) and Important Entities (IE). Providers of social networking services platforms (Article 4(22), NIS 2) are included in the Digital Services sector, in the IE category. Providers of telecom services are included in the Digital Infrastructure sector in the EE category. However, according to the EECC, the definition of electronic communications services includes interpersonal communications services[6], including most OTT services. This implies that providers of social networking services platforms could fall within both the scope of EE as well as IE. Whether small or micro entities (SME) providing social networking services platforms should be included in NIS 2 at all is unclear. If they are an IE the answer is no; if they are an EE within

[6] Article 2(4)(b), EECC.

the meaning of Article 2.2(a)(i), the answer is yes. Moreover, the question of what kind of supervision these entities are under (*ex ante* or *ex post*) would also be unclear.

NIS 2 is in need of clarification regarding how to distinguish between these two possible categorisations of providers of social networking services platforms. Additionally, there could be confusion regarding the status of certain cloud services. The service Zoom might, for example, fall under both the cloud service definition as well as the telecom service definition as an OTT.

Additional clarity on certain definitions

The following are examples on where more clarity would be beneficial:

DNS Services

Recital 15 of NIS 2 states that all DNS services should be included in the scope, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers. In Article 4(13)-(15) all services mentioned in recital 15 are included in the definitions, except for the root name server. As this is such an important part of the DNS resolution chain, the Commission should consider including it in Article 4 (e.g. as part of the DNS service provider definition), and not only in a recital.

Near misses

Throughout NIS 2, four similar concepts are used to describe issues, or would-be issues, in services: incidents, cyber threats, vulnerabilities and near misses. The first three are included in Article 4 with their own definitions, while 'near misses' is only defined in recital 39. As the distinction between these four terms could prove difficult for many, the Commission should consider including the 'near misses' definition in Article 4.

Data centre services

The definition of data centre service in Article 4(20) contains a substantial enumeration of what subservices must be included in the main service for it to be within the scope of NIS 2. The provision lists "centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control". If an entity provides all these services but one, they will likely fall outside the scope of NIS 2. The Commission should consider putting "or" instead of "and" between some or all of these services to ensure that all entities that are intended to fall within this scope do.

3.3. Jurisdiction

Article 24 states that certain specific service providers shall be under the jurisdiction of the Member State in which they have their main establishment in the Union. It is further specified that "main establishment" shall be where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be where the entities have the establishment with the highest number of employees in the Union.

In the current NIS Directive, the digital service providers have the same kind of regulation as stated above regarding jurisdiction, with the exception that there are no guidelines as to how to interpret the "main establishment" provision. As has been apparent in many of the Work Stream 5 (WS5) working papers, the question of jurisdiction has caused a lot of confusion regarding how to interpret the provision. This confusion has in some cases led to Member States not applying the NIS provisions on security and supervision. Extending this type of provision to additional entities might carry those issues into the interpretation and application of the jurisdiction for those entities, even if clarifications on how to interpret "main establishment" have been made in the NIS 2 Directive. In detail, PTS has the following main concerns about this Article:

1. The proposed jurisdiction will prove difficult for the Member State in which an incident occurs when the main establishment is not located within that Member State. If supervision activities need to be carried out for an establishment that is located in a Member State under which jurisdiction it does not fall, the competent authority (CA) or correct supervisory body (SB) will need to ask the SB in the concerned Member State to carry out the activities for them. The intention is for SB's to have a harmonised and cooperative approach to cross-border supervision, in accordance with Article 34. In practice, however, this type of jurisdiction will likely prove difficult or at the very least make the supervisory process move slower than if the entities were under the jurisdiction of the Member State in which they provide their services or are established, i.e. where the incidents can occur. Thought should be given as to whether this provision causes more problems than it solves. However, if this becomes the jurisdiction provision in the final NIS 2 Directive, the details of how to carry out the cooperation according to Article 34 must be clearly defined for all Member States.

2. An entity shall be deemed to have their main establishment in the Member State where the decisions related to the cybersecurity risk management measures are taken. This provision might result in difficulties in application. It is possible that different establishments, all connected to the same entity, take different risk

management measures and that these are locally or regionally governed. The wording "decisions related to the risk management measures" could include a variety of decisions made in a company and it is unclear which kind of decisions the provision is intended to entail. The provision implies decisions regarding specific actions and activities, rather than overarching policies for the entity as a whole. When it comes to groups of companies, the assessment of where risk management measure decisions are taken could prove difficult and arbitrary. If this becomes the final provision in the NIS 2 Directive, clarifications are needed regarding the type and level of decisions that are intended within the frame of the Article.