ECS

EUROPEAN CYBER SECURITY ORGANISATION

POSITION PAPER
The NIS Directive Review

WG3 I Users Committee

NOVEMBER 2020

www.ecs-org.eu

Position Paper on the NIS Directive Review

ECSO Users Committee

DISCLAIMER

The suggestions of this paper, proposed by private users & operators members of the ECSO Users Committee, do not represent the position of Member States and public administrations members of ECSO.

Introduction

With the upcoming revision of the NIS Directive – Ares(2020)3320999 (NISD) expected to be finalised by the end of 2020 following a wide public consultation, the ECSO Users Committee would like to present its suggestions and expectations for the updated NISD 2.0[1] while highlighting the limits and challenges of the current version complementing and / or reinforcing certain comments provided to the Commission by single ECSO members.

It is clear that the overarching objective of the NISD aims to achieve **a common level of security across the Member States (MS) while balancing the requirements from different sectors**. However, the lack of specific criteria for MS to apply at the national level has led to **fragmented approaches in defining specific security measures and in identifying Operators of Essential Services (OES), thus limiting the effectiveness of the Directive.**

Ever since NISD entered into force in 2016, Users and OES in the different sectors and subsectors covered by the Directive have noticed a significant increase in the level of risk of cyber incidents, and it is now crucial that the revision of NISD tackles the evolving challenges of cybersecurity towards a more cyber resilient Europe.

On the outcomes of the NIS implementation:

Before deep diving into the specificities for OES and incident reporting, it is important to stress a fundamental aspect of cybersecurity: the NISD 2.0 should cover all actors of the specific verticals **including the smallest**

[1] For the purposes of this document, we use NISD 2.0 to denote the revision of the current NIS Directive or replacement thereof with a new legislative act (depending on final inter-institutional agreement)

ones, as vulnerability comes from the weakest link in the chain. The NISD, even if addressing in particular main companies as OES or DSP, has an indirect impact on the entire supply chain (and hence the SMEs) providing solutions to those main companies.

This approach would **ensure a level-playing field** between actors of at least the same sector, if not cross-sector, as well as a **higher cyber resilience** as a whole and therefore **ensures the resilience of services from end-to-end** as expected by consumers.

When it comes to cyber resilience, **the NISD does not address the operational aspects of enforcements** either, i.e**. supporting the OES when managing and responding to cyber-attacks especially in times of high demand and crisis. More supportive measures for the private sector** would be expected for cybersecurity at the European level when fighting against cyber-crime. This is an area that **not only requires legislations but concrete rules** to be followed and ensure their effective implementation and use.

Some requirements of the NISD came as **additions to already existing requirements** set out by different regulations, which is **a burden for Users/OES in the involved sectors**. The extension of incident reporting and security requirements to different sectors is a good starting point for a common level of security of network and information systems. However, in some sectors, such as financial services for example, which are already heavily regulated, **the NISD added a further compliance burden instead of harmonising legislations and procedures.**

On the Operators of Essential Services (OES):

The overly **flexible implementation of the NISD by MS led to a high level of heterogeneity in defining and identifying OES at the national level**. This is especially evident in the European Commission's own report on 'assessing the consistency of approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems" issued in October 2019[2]. A similar **lack of harmonisation was also applied to the security requirements and controls.**

These statements can be verified with the available, and heterogenous, national repositories. **Bringing a harmonised definition for the identification process of OES across MS** is the very first crucial point that should be tackled by NISD 2.0, while keeping in mind that some MS already have identification measures of critical services at national level and specific security requirements. The aim would be **overarching rather than overlapping and over-burdening.**

[2] European Commission (2019), COM(2019) 546 final, REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0546&from=EN

On incident reporting:

Given the current stage of implementation of the NISD, introducing new requirements could become a burden for some sectors and prove to be difficult to implement for other sectors. Rather, the review should focus on **harmonising its implementation** across Europe and **extending its scope to all actors of each of the tackled sectors, while considering other regulations and directives.**

I**ncident notification requirements should be better streamlined** to allow for more efficient incident reporting, through a **better degree of alignment**, in particular for **incidents with a cross-border dimension to improve the value of the transferred information**. As such, the updated **NISD could define a single template** for reporting that takes into account all the different incident reporting requirements specified in EU regulations. For instance, Operational Indicators of Compromise coming from European Institutions or other Member States would be particularly useful in this case. Therefore, NISD 2.0 should organise sharing practices between all involved actors.

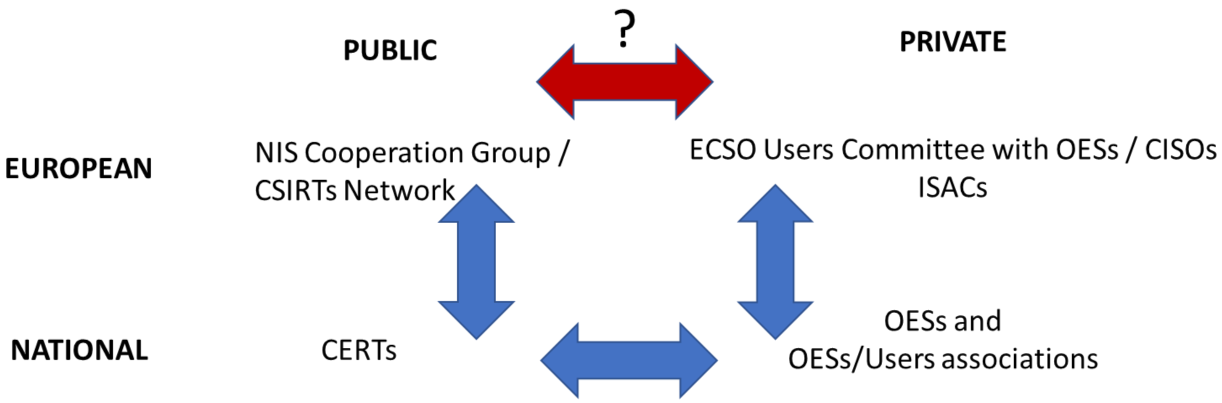
On information sharing:

To support information sharing at European level, ECSO created the Users Committee (see Annex). This Committee is gathering of CISOs from the main members (those having a major impact as OESs even beyond the perimeter of the NISD but having a critical role at national and European level). With its Users Committee, ECSO is thus already **building up a complementary tool** to what the future NISD could envisage.

Two years ago, ECSO also issued a paper supportive of the creation of ISACs for trusted information sharing but offering some recommendations to improve the “traditional” ISAC model. More recently, our Users Committee also revised its position on the topic, and while considering **ISACs as an interesting tool to start a dialogue between public and private and/or across private bodies in the prevention and recovery phases**, yet it considers that their effective added value at European level is limited when dealing with operational crisis management. The excessive mix of stakeholders as well as the complexity to link ISACs from different sectors with information from different MS has shown the **difficulty to enlarge to all these stakeholders the mutual level of trust and allow strategic sharing of information among key decision makers at European level especially during crisis periods**. The **ECSO Users Committee would thus be a complementary tool** also to cover this gap at European level also suggesting a **close cooperation with European and national administrations to support the work of the “Blueprint” for fast responses,** today only based upon a public-public cooperation.

We understand that the NISD as legislation is addressing national public administrations but its **impact is mainly on the private sector** which is the owner and is providing those essential and digital services mentioned in the Directive and which is facing every day those threats considered by the Directive. More attention should be paid to the needs of the private sector also during the implementation and operation phase of the reviewed Directive. For these reasons, **public – public agreements on measures to be taken, could not necessarily satisfy the needs and the implementation / use by private OESs**.

The European Commission could facilitate information sharing between stakeholders and OES at European level by putting in place a dedicated structure based on mutual trust and voluntary participation, in closer link with the NIS Cooperation Group and the CSIRT Network. In turn, it would create a **no-blame culture by encouraging public-private partnerships with the additional support from the authorities that can be seen as liability exemption factors and incentives to share**. In this way, the authorities would have all the relevant information for supervisory purposes, while leveraging public-private associations as the focal points for information sharing and to having **a role of mediation between institutions/authorities and the private sector that they should support.** It is worth mentioning that the Italian bank, Intesa Sanpaolo, and the French energy OES, EDF (Electricité de France), in their recommendations as chairs of the Users Committee have suggested **ECSO for such a role**.


?
PUBLIC
PRIVATE
EUROPEAN
NIS Cooperation Group / CSIRTs Network
ECSO Users Committee with OESs / CISOs ISACs
NATIONAL
CERTs
OESs and OESs/Users associations

Indeed, the ECSO Users Committee has identified and recently published a green paper on the existing information sharing structures and their limitations. Most current settings encourage information sharing from public entities to other public entities, or from national private entities towards their national public administrations, or among private entities of the same sector. The missing settings remain at the level of European cross-border and cross-sector cooperation, which are the main objectives of the Users Committee. This requires not only a **public-private cooperation at the European level, but also private-private cooperation across all sectors.** After all, cybersecurity is a horizontal topic, and so should be information sharing.

***On the future and next steps*:**

Reviewing the NISD should aim at harmonising the whole ecosystem using regulations that already exist for some sectors and extending them to all other sectors in all MS, while at the same time **aligning security levels**. It is important to keep in mind that the management of multiple incident reporting requirements require heavy costs that some sectors cannot necessarily cover**. A level-playing field between MS and all the actors of the same sector is still needed to ensure equity in terms of costs**.

Such an endeavour requires the input and full participation of all actors and stakeholders. So far, the NISD has entirely focused on MS, i.e. national public administrations. If NISD 2.0 is to bring an added value towards a harmonised ecosystem, then **the NIS Cooperation Group also needs to include and actively engage with the European private sector**. All the challenges and recommendations issued in this paper can only be tackled via a **holistic and collaborative approach from all stakeholders, public and private alike.**

Finally, a particular focus should also be put on the **emerging technologies and recent technological developments which enhance the vulnerability of certain actors**. Once again, while a careful consideration should be put into harmonising legislative requirements, NISD 2.0 should not add further compliance burdens if they are already regulated by other pieces of legislation at the European level.

About ECSO's Users Committee (UC)

In September 2018, ECSO created its Users Committee (UC), a European transversal (cross-border and cross-sector) committee where Users and Operators of Essential Services (OES) can share sensitive information and strategic intelligence on cyber threats in a confidential and trusted way. The UC itself is autonomously attached to ECSO's Working Group 3 "Sectoral demand" that represents Suppliers, Users and OES from different sectors – industry 4.0, energy, transportation, finance, public services/e-government, healthcare, smart cities, and telecom/media/content.

The UC members are restricted to a network of European Chief Information Security Officers (CISOs) (or equivalent) who provide strategic suggestions from a private sector and strategic operational perspective in order to tackle current and future challenges and needs for the cybersecurity solutions providers (CSSP) and more widely the cybersecurity market.

Indeed, it is our understanding and approach that Users and OES are the drivers of all activity on the European cybersecurity and digital market, and while a dialogue with the public sector already exists, often at the national level, a complementary dialogue with the private sector is also necessary to create a direct impact at the European level. Users/OES are key actors in the field of cybersecurity, especially since CSSP (the offer) can only offer tailored products based on the needs expressed by the Users/OES themselves (the demand).

Based on these elements, the UC has a quadruple approach to its portfolio of activities:

- A network of European CISOs (or equivalent) across sectors and across borders
- An open forum of exchange and discussions for lessons learned and best practices
- A trusted and confidential environment for strategic intelligence sharing among peers
- Understanding of the needs, requirements, and challenges of a CISO and conveying these messages to the right actors

ECS

EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

29, RUE DUCALE - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE : WWW.ECS-ORG.EU