Reference document on Incident Notification for Operators of Essential Services

Circumstances of notification

CG Publication 02/2018

NIS Cooperation Group
February 2018

ABOUT

This document has been drafted and endorsed by the NIS Cooperation Group members.

The Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security ('ENISA'), has been established by Article 11 of the Directive (EU) 2016/1148 'concerning measures for a high common level of security of network and information systems across the Union' (NIS Directive). It facilitates strategic cooperation between the Member States regarding the security of network and information systems.

Contents

1 Introduction

1.1 Background

The NIS Directive is the first piece of EU legislation specifically aimed at improving cybersecurity through-out the Union. This in itself represents a very significant step in the approach to securing EU information systems.

By ratifying a definite number of obligations across the EU, the Directive will help ensure a consistent approach to cybersecurity 'with a view to achieving a high common level of security of networks and information systems within the Union so as to improve the functioning of the internal market'.

The NISD represents the most ambitious piece of EU legislation regarding cyber security, with the overall purpose of enhancing cyber security in all 28 EU Member States. Implementing such a large and complex legal initiative, that directly affects stakeholders from multiple industries and even different continents we do consider that several prerequisites have to be accomplished at national level before imposing the regulation.

The NISD provides a clear justification for the necessity of such provisions, as stated in recitals 1 and 2: "network and information systems play a vital role in the society […] essential to economic and societal activities, and in particular to the functioning of the internal market" and "the magnitude, frequency and impact of security incidents are increasing". By imposing incident notification requirements at national and EU level one can be able to better identify the challenges within the sector and propose relevant mitigation measures, based on facts and figures.

With a view of fostering mutual understanding of challenges related to the implementation of key provisions of the Directive and of supporting convergence of national approaches to their implementation, a Cooperation Group (CG) is established to facilitate exchange of information and best practices among Member States.

Taking advantage of this possibility and upon proposal from the European Commission (EC) a group of voluntary Member States' experts (hereinafter: "the Work Stream") was therefore established within the framework of the Cooperation Group with the support of ENISA, in view of exchanging views on the issue of incident notification for OES.

The present "reference document" sums up the Groups' main findings and non-binding recommendations.

1.2 Purpose

Recognizing the solid and growing risk posed to OES and their potential impact on EU's economy and society and taking into account that some OES may be established in different EU Member States, the Group agreed that all may benefit from coherent approaches to the transposition of the NIS Directive with regard to incident notification for OES.

The Group also considered the need for Member States to be provided concrete and immediately usable recommendations to support their transposition process, instead of favouring an inclusive expert approach, which would have taken an excessive amount of time and would likely not have been produced before the deadline for the NIS Directive transposition.

As a consequence, as indicated in Article 14(7) of the NIS Directive, the Work Stream aimed at offering indications on how Member States may today address the transposition of article 14 (3) and (4) of the NIS Directive related to incident notification for OES. It has to be noted that this is a living document and it will continue to be updated and improved based on the state of the art threat landscape and the decisions taken by the Group.

2 The NISD incident notification scheme for OES

2.1 Prerequisites of a successful incident reporting scheme

By having incident notification requirements at national and EU level one can be able to better identify the challenges within the sector and propose relevant mitigation measures, based on facts and figures. As any other policy implementation processes there are certain issues that need to be taken into account by responsible authorities before proceeding. Among the general and specific prerequisites, we can mention:

1. Provide the proper justification for the new policy:

   Develop a strong, coherent and easy to understand message explaining the necessity and importance of the notification requirements. Just mentioning "EU legal framework compliance" will not help as some stakeholders' level of awareness is not sufficient at the moment. Network and information systems and services play a vital role in society. Cyber incidents are part of nowadays reality. Their reliability and security are essential to economic and societal activities.

2. Maintain a permanent public-private dialogue:

   As the requirements affects both public and private stakeholders, maintaining and further strengthening cooperation with these partners will help develop and implement more effective and suitable policy. Firstly, as these partners have the experience needed and secondly involving them in the developing phase and raising commitment in the implementation phase. Listening to their concerns and adapting the policy to their needs also (as much as possible) can be a critical success factor. An example is the determination of the thresholds for incident reporting. This differs per sector, operator and service.

3. Building trust and providing incentives for reporting:

   The objective of the policy (at least in the current scenario and phase) should be to collect incidents in order to offer assistance and better understand the challenges within the sector. Penalties should not be the main focus, but should not be excluded also.

   A successful implementation also depends on the commitment of the stakeholders to the process. Providing incentives might be a good solution. For example, providing incident response coordination (by a responsible authority or National CSIRT), provide periodic analysis of collected incidents and identify main trends, periodic feedback to the industry on the status and actions taken etc. Providing warnings and situation reports for OES generates added value. Another example is to ensure a strict regime regarding the handling of confidential information to a third party. For the release of confidential information that could be traced back to an operator (name of the operator, etc.), a special public disclosure arrangement that supersedes the Government Information (Public Access) could be added.

4. A proper regulatory/institutional framework in place

   As soon as the incident reporting policy is adopted there should be in place a proper process to follow when reporting and also a coherent institutional framework. Operators should be aware how to report and what to include in the notification.

   The terms under which the notification must be made have to be simple and clear and the means/tools to do it have to be secure, reliable and easy to use. Therefor it might be helpful if MS would give OES examples for reporting worthy incidents.

Simultaneously a proper institutional framework must be in place. Operators have to be aware to whom to report to and at what time. Usually cyber related incidents tent to produce multiple damages to many types of assets (equipment, data, services etc.) and the probability they go beyond the limits imposed by the NISD (touching on privacy issues maybe) is high. In this respect having a single point of contact at national level for incident notification, as required by the NISD, might ease the situation by simplifying the reporting process. Also transparency and feedback is important.

5. Monitor, review and evaluate the overall implementation:

   Periodic review and improvement is necessary. As cyber security challenges landscape is on a permanent change, the incident reporting policy in place has to follow the same approach. Periodic reviews of parameters used, thresholds and other variables are necessary for a successful implementation.

6. Use already existing good practices defined within the industries:

   Most of the sectors defined within the NISD are well-developed, with a history that goes beyond the informational age. Although the concepts of essential services and critical infrastructure are newly defined, their core role of those sectors remains the same, notably to provide vital services to the society. Safety standards, regulations and incident reporting schemes have been already developed in most of the traditional sectors (energy, transport etc.) with a focus on the continuity of the services provided. In the past years cyber has been added as an extra threat which needed special attention, but following the same procedures and policies already in place. Cases where the policies had to be fully redrafted due to cyber are very rare, mostly cyber was added as an extra module to what was already there. In this respect identifying and tapping into the existing procedures/policies can save a lot of time and also assure the continuity of regulatory effects resulting from previous legislation.

2.2 The NISD incident notification provisions

The incident notification requirements for OES are defined within Art. 14 points (3) to (7). The incident notification process should be in line with the following requirements, as extracted from the articles mentioned above:

- Competent authorities/CSIRTS in place for the purpose of the notification: Every Member State should appoint competent authorities or CSIRTS to which the OESs will notify significant incidents.
- Identification of OES: OES should comply only in cases where incident concerns the provision of the essential services. The NISD covers incidents affecting network and information systems used in the provision of essential services.
- Significant incidents should be reported: All significant incidents that affect the continuity of the essential services provided must be reported without undue delay.
- Cross border impact must be notified: The responsible part, either the competent authority or the CSIRT (art. 14 (5)), shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications as referred to in the first subparagraph to single points of contact of other affected Member States. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident.
- Determine significance: In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:
  - (a) the number of users affected by the disruption of the essential service;
  - (b) the duration of the incident;
  - (c) the geographical spread with regard to the area affected by the incident;

The Directive does not restrict the usage to only the 3 parameters above. In this respect several other parameters might also be used, depending on national specificities and particularities of each sector. NISD provides also a set of parameters for the purpose of the identification of OES (Art. 6) that could also be useful in the context of the reporting process:

  - (d) the dependency of other OES sectors on the service provided by the affected entity;
  - (e) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;
  - (f) the market shares of that entity;
  - (g) the geographic spread with regard to the area that could be affected by an incident;
  - (h) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

- Follow-up after notification: the competent authority or the CSIRT shall provide, when the circumstances allow, the notifying operator of essential services with relevant information such as information that could support the effective incident handling.
- Informing the public: After consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident.
- Guidelines can be adopted by the CG: Competent authorities acting together within the Cooperation Group may develop and adopt guidelines concerning the circumstances in which OES are required to notify incidents, including on the parameters to determine the significance of the impact of an incident.

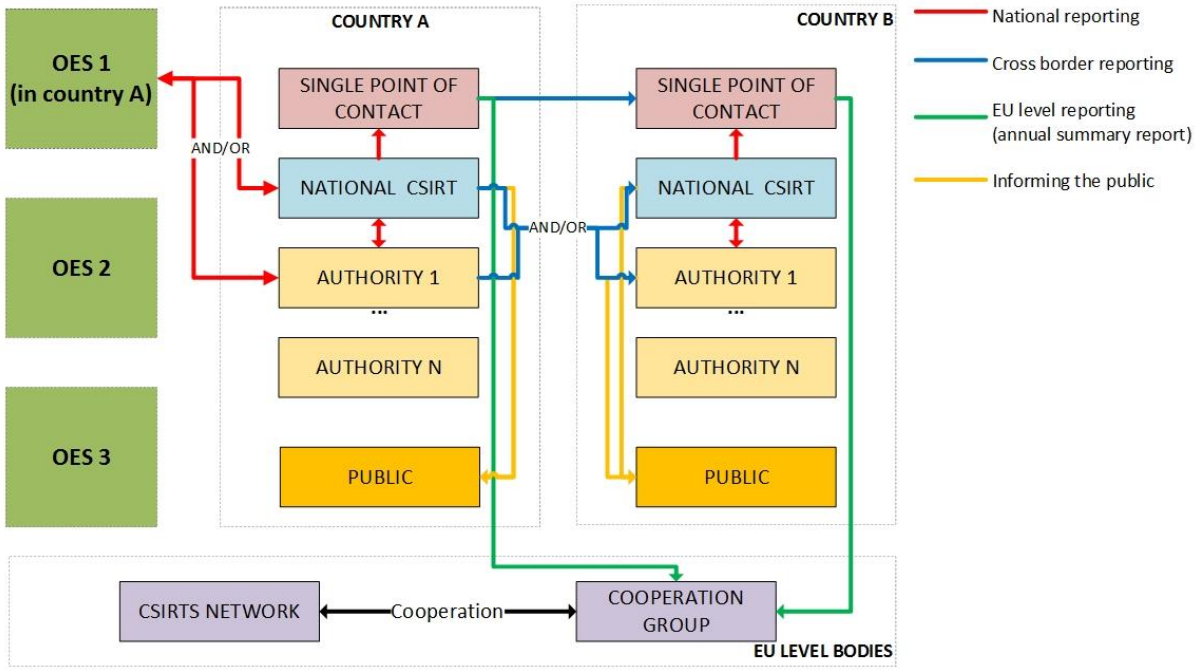

Figure 1 Overview of the incident reporting process for OESs

2.2.1 Possible institutional set-ups at national level

The NISD Directive sets the general framework in terms of reporting without going into details on how things should be organized at national level. In this respect MS have the liberty to choose their own national organizational set-ups.

The following set-ups where identified within our research as most used by MS:

1) **Incidents are reported only to one single national authority** (e.g. National CSIRT or Single Point of Contact which is in the same time the NIS competent authority). In this case the authority has a clear view on all incidents and can swiftly react. The drawback of this approach is that one single authority usually does not have sector level experience for all domains regulated by the NISD. In this case the authority can ask support from sectoral authorities and share incident data with them. As mentioned throughout this document, sector level experience is crucial in dealing with incidents.
2) **Incidents are reported to sectoral authorities.** In this scenario the sectoral authorities (e.g. regulators of CSIRTS in Energy) will receive the incidents from the operators. The single point of contact will act as a central hub where all incidents are collected, being in permanent contact with the incident-receiving authorities. A good cooperation between involved authorities is very much needed in this scenario.
3) **A mix of the two set-ups above**. MS may opt for hybrid set-ups where one authority covers multiple sectors, but some sectors have sectoral authorities.

2.2.2 Notification timeline

In terms of timing of the notification, most of the MS have indicated the use of a two phase or three phase reporting: a preliminary reporting, an intermediate reporting and a full reporting. The only requirement that the NISD imposes in terms of timeline is stated in art. 14(3) that "member States shall ensure that operators of essential services notify, without undue delay". The meaning of "undue delay" might be as soon as the operator is aware of the significant incident, as soon as the triggering event occurs (e.g. a cyber-incident leaving 1 million people without energy might be the trigger for the notification, even though not all details are known soon after the blackout).

The first notification (preliminary) should be done as soon as possible, even when not enough information is available. The purpose of this initial reporting is to raise the authority's awareness about the incident and possible consequences. Due to the lack of sufficient data the operator can use forecasts and assumptions based on previous available statistics. Nevertheless, this approach has to be clearly mentioned in the notification.

Intermediate reports have to be sent periodically or when new information is available. This type of reporting has the purpose of updating the authority upon the status of the incident. Not many MS have mentioned the intention to use this phase.

The closure of an incident should be followed by a full report, where all data required by the authority are submitted. The second phase might come much later (e.g. weeks, months) than the previous, as soon as the operator has collected all necessary data in order to provide a full overview of the incident. It is recommended that the authority keeps contact with the operator in cases where the investigation could take a very long time.

2.3 Types of incidents covered by the NIS Directive

Defining the scope in terms of types of incidents to be covered is difficult as long as terms are not properly clarified and there is no direct mention in the legislation. In order to help the stakeholders involved to get an accurate response to several issues that might arise during the implementation of the NISD, various definitions and provisions must be revisited. Therefore, in the following, we will try to summarize the basic applicable concepts.

As mentioned by the NISD (Art. 4 - definitions) an ***incident*** "*means any event having an actual adverse effect on the security of network and information systems*".

Similarly, article 4 (1) defines the ***network and information systems***, by which we understand *interconnected systems that process, transmit and store data* so as to provide a digital service.

Further, ***security of network and information systems*** is defined as the "*ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems*". The NISD focuses only on these four protection goals; nevertheless, MS are encouraged to go more in case needed (e.g. accountability).

On the other hand, ***adverse effect*** is a concept not defined within the Directive. Nonetheless, we can consider the general meaning of the words: preventing success or development, harmful, unfavorable[1].

In addition to the definitions above, a notion that needs clarification is ***significant impact***, a concept that clearly marks the starting point of incident reporting activities. The notion is used in Art. 14 (3) that states that OES will have to "notify, without undue delay […] incidents having a significant impact on the ***continuity of the essential services they provide***.". Furthermore, the Directive indicates that significant impact must be determined based on 3 parameters (explained in subchapter 2.4).

A definition regarding the continuity of service is missing from the NISD, but it is our understanding that in this particular context, where the essential services are critical for societal and/or economic activities, continuity should be understood as the ***provision of a service at an agreed/reasonable standard of quality***. For example, in the case of the Drinking Water subsector, the lack of water due to cyber issues certainly represents an incident, but also the improper provision of water (due to cyber issues) in terms of quantity, quality (health) or other relevant parameters. In conclusion CONTINUITY does not mean only availability but the proper provision of the essential service, a term that is usually assimilated in practice with business continuity. ISO 22301 provides a comprehensive definition of business continuity as "***capability of the organization to continue delivery of products and services at acceptable predefined levels following disruptive incident***".

By combining the notions highlighted above it is possible to develop a comprehensive idea about what types of incidents should be considered within the context of the NISD-OES. An overall definition can be summarized as follows:

NISD incident = Any event affecting the availability, authenticity, integrity or confidentiality of networks and information systems (used in the provision of the essential service), that has a significant impact on the continuity of the essential service itself.

[1] https://en.oxforddictionaries.com/definition/adverse

Note: For the rest of the document, for simplicity, we will refer to availability, confidentiality, integrity or authenticity, as the 4 properties or protection goals that a network and information system used in the provision of essential services must assure under the NISD.

It is to be concluded that the effect of an incident must be a disruption in the essential service that is being provided, due to a cause concerning the underlying IT/computer system used to assist the provision of the service. In this respect the disruption of the essential services must be described based on the specific performance parameters of a particular industry (e.g. reduction of a power generating facility, incidents regarding the load in the network both measurable in MWh;). Almost all industries within the NISD are mature, operating for a very long time and already having in place parameters to measure the performance of the services offered. Whether it is related to crisis response, safety regulations or other areas, major industries have methods of defining significant incidents regarding the essential services offered. In this respect we can conclude that the identification/detection of the significant incidents should start from the specific situations considered as crises within different sectors and subsectors.

NOTE regarding other types of useful data:

The NISD covers incidents that have a significant impact upon the continuity of the services provided. But, as this is one of its objectives, it is expected that the NISD will significantly improve the resilience and reliability of OES services over time by shortening incident impact and remediation time and reducing the impact upon the population. It also desirable that the authorities have a complete picture of the risk level within sectors. In this respect they have to be aware of the threat landscape and potential weaknesses in the operator's systems. With less incidents reported their visibility within those areas will decrease, and this might impact the quality of the regulatory and policy making process.

In order to tackle this situation some MS have taken the initiative of also requiring notification ***of events that can possibly have a significant impact*** upon the continuity of the service. In some cases, these incidents can materialize as vulnerabilities in their services/infrastructures or just incidents that have been handled efficiently without provoking significant damages.

Likewise, ***voluntary incident reporting*** is also a good initiative, as it might help the authorities having a complete picture on the risk level within one sector.

Relying only on data submitted from incidents might not offer full visibility on the risk level for sectors or even operators. The authorities need to incorporate as much additional data as possible from different other sources (cooperation with public administration bodies at regional level, inter-sectoral cooperation, public data on incidents and vulnerabilities, etc.)

2.3.1 Exploring synergies with other EU incident reporting schemes

In recent years the EU has made significant progress in terms of cyber security related regulation. Starting with scattered initiatives in certain sectors (e.g. Telecom), the EU related legal landscape has evolved a lot to the point of an EU wide Cyber Security Strategy and the NISD. Although, the number of legal initiatives touching on cyber security might be bigger, we will try to depict below the ones that might have a tangible impact on the NISD incident notification requirements.

1. **The Telecom Package** represents the EU's regulatory framework for electronic communications, and is, according EU Commission's website, "[…] *a series of rules which apply throughout the EU member states. It encourages competition, improves the functioning of the market and guarantees basic*

user rights". The Telecom Package was adopted in November 2009. Art. 13a, of the Directive 2009/140 EC aims at ensuring the security and integrity of electronic communication networks and services, dealing mostly with prevention of outages or service disruptions (availability of the service). This is partially achieved through requiring telecommunication service providers to take the appropriate technical and organizational measures to manage the risks posed to security of networks and services, guarantee the integrity of their networks (ensure the continuity of supply of services provided over those networks) and ***notify the competent national regulatory authority (NRA) of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services***.

Currently there is a mature incident reporting framework at EU level covering the notification of significant incidents above certain thresholds. According to Art. 1(3) of the NISD the security and notification requirements shall not apply to undertakings which are subject to the requirements of Articles 13a and 13b of Directive 2002/21/EC (Telecom Framework Directive). However, the market reality is that these undertakings do provide the specific services such as Domain Name Systems (DNS) or Internet Exchange Points (IXP) covered under Annex II point 7 of the NIS Directive. Therefore, these undertakings will be subject to notification requirements of the NIS Directive in relation to the provision of these particular services. However, given the fact that DNS service providers are specifically mentioned in the NISD, but not in the Telecom Package, it would be beneficial to develop synergies between the two incident reporting mechanisms. Synergies are particularly important in light of the fact that every Internet Service Provider (ISP) needs at least one DNS server to provide its services. Moreover, incidents concerning DNS services that belong to ISPs are already happening and they are reported currently under the Art. 13a incident reporting scheme.

2. **eIDAS Regulation -** The new regulation for electronic identification and trust services (Regulation (EU) No 910/2014, referred to as eIDAS), contains Article 19 which requires, among others, that providers of trust services 1) assess risks, 2) take appropriate security measures to mitigate the risks, and 3) notify the supervisory body about significant incidents/breaches. In this case an EU wide incident reporting scheme is also in place and 2017 was the first year when ENISA received incidents. Although the relation between eIDAS and the NISD may not be so obvious, there is certainly a link between them. Digital certificates are frequently used as authentication factors in financial services, cloud providers or other services that may fall under the NISD. Any security incident affecting the trust services used as authentication means within the essential services might also affect the continuity of the essential service itself.

   As both regulations are considered without prejudice, according to Art. 1(3), the MS should pay attention when defining the national policy in this case.

3. **The EU General Data Protection Regulation (GDPR)** replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. Section 2 art. 32-24 provides requirements as regards the security of personal data and art. 33 sets the ground for notification of personal data breaches to supervisory authorities. Although there is a clear theoretical line that can be drawn between the scope of the two initiatives, in practice, data breaches accompany almost every major cyber incident especially in industries where the provision of the service is strictly digital (finance, cloud, online market places etc.). Overlaps between NISD and GDPR in terms of incident notification are not excluded and MS have to be aware of them. A good example in this case might be the attack on the Sony PlayStation Network in 2011, a data breach that led also to a loss of service availability.

As both regulatory acts are considered without prejudice the same incident might trigger notification requirements under both pieces of legislation. MS should pay attention in this case when defining the national policy and possibly work at the development of synergies between different incident reporting mechanisms, with a view to streamlining the notification process and simplifying compliance for stakeholders.

4. **The Directive (EU) 2015/2366 (PSD2)** provides a regulatory framework for payment services in the European market. Among other provisions, it defines requirements for effective incident management procedures (art. 95) and incident reporting (art. 96). Payment service providers, "*shall report without undue delay any major operational or security incident* to their competent authority in the Member State. In accordance with art. 96 (3) a full incident reporting guideline containing details on classification of major incidents, the content, the format, including standard notification templates, and the procedures for notifying such incidents along with criteria on how to assess the relevance of the incident by competent authorities has been published by ECB and EBA. The Guidelines will apply from 13 January 2018. Payment services are also part of the financial services sector within the NISD.
5. **Safety related regulation** – most of the traditional industries (energy, transport, finance) that provide essential services are heavily regulated, on many aspects of their activities. Safety is one of the areas under extreme regulation by national authorities, regional organisations or international treaties. Due to the intense interdependencies between operators that offer the same services (electricity providers depending on other electricity providers) and among sectors (transport relying on energy) and due to the high risk to safety of human lives that any disturbance of their services might bring, these regulations have become a must. Any kind of disturbance in the provision of their services can cause damages to human lives or economies and in this respect those industries have acquired some expertise over the years in terms of information exchange, incident reporting, crisis cooperation etc.

   Cyber incidents can also be among the causes affecting the proper continuity of the service. As the NISD applies only to the 28 MS of EU, certain precaution must be granted to existing safety regulation in place that might apply beyond political borders of EU.

   It is our understanding that the development of any NISD incident notification scheme must take into account any national, regional or international incident notification schemes concerning the sectors, especially in the safety area. You can find more details in the sectoral annexes (A).
6. **Law Enforcement related requirements** - Directive 2013/40/EU on attacks against information systems has the objective to approximate the criminal law of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities. Cyber-attacks can also cause NISD incidents. Although the correspondence here is obvious MS have to take into account also the potential involvement of law enforcement agencies in the post-incident investigations. When designing incident notification policies particular attention must be granted to the overall incidents handling and reporting procedures so that important evidence is retained in case of an investigation. More cooperation between law enforcement agencies and responsible authorities is desirable in this case.

Drawing a line between all reporting requirements above is possible, but only in theory. In practice, an incident can fall under many categories and under the responsibility of many authorities. It is up to the MS to benefit from these synergies and define a proper national policy taking into account all constraints and

opportunities so that an overall “friendly” and easy-to-use incident notification scheme would be put in place.

An initiative regarding a Common Notification Platform at national level that will collect incidents from multiple schemes (and authorities) have been proposed by one MS. The platform will act as a clearing house where many authorities can share information about incidents. The existence of such platforms is highly encouraged as it can reduce the burden both for authorities and also operators.

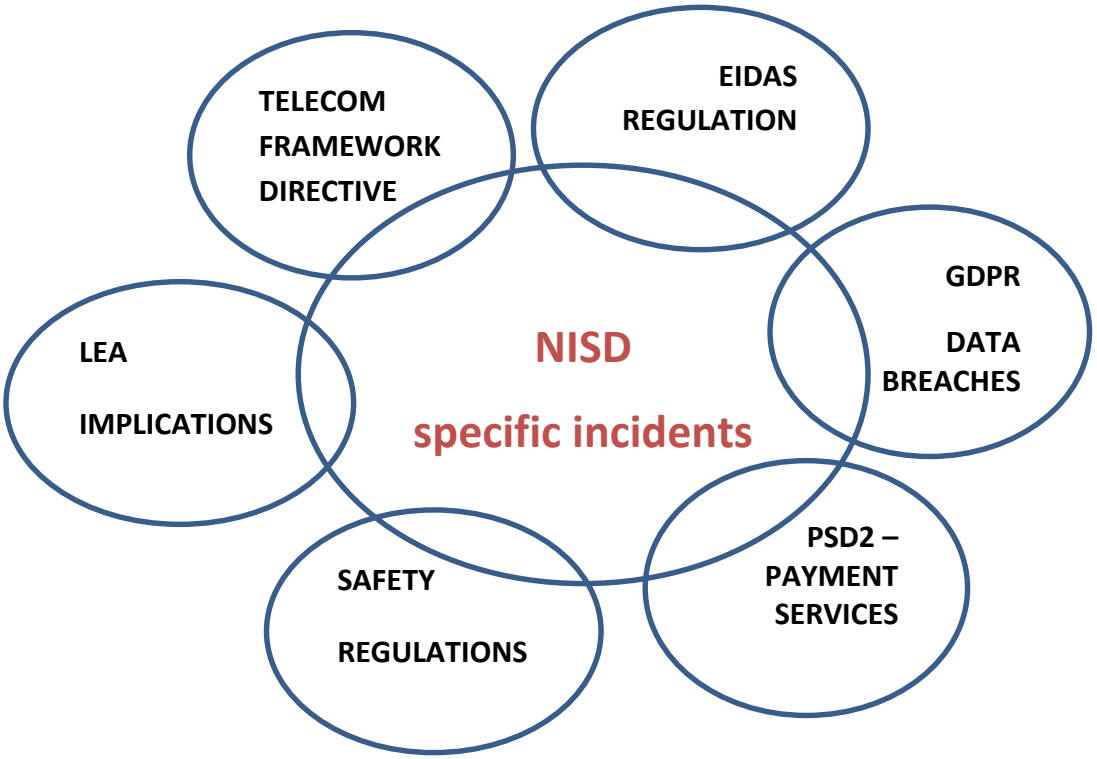

Figure 2 Exploring synergies NISD and other incident reporting schemes

2.4 Determining substantial incidents

Art. 14 (4) of the NISD mentions specific parameters that have to be taken into account when defining the significance of an incident. According to art. 14 (4) the following parameters in particular shall be taken into account:

(a) the number of users affected by the disruption of the essential service;
(b) the duration of the incident;
(c) the geographical spread (area affected by the incident);

The underlying objective of the NIS Directive is to improve the functioning of the internal market through resilience/cybersecurity and especially incident notification. The achievement of this objective implies the use of some generic criteria that can be applied to the broad range of industries that have to comply.

Applying criteria concerning society as a whole seems like the right approach in this case, but raises some issues for the operators. Measuring the significance in terms of impact on society forces the operators to involve additional analyses within their incident handling procedures. Most of the operators from different sectors mentioned that the measurement of this kind of impact was not part of their usual business.

As significance needs to be measured accordingly operators have to translate damages to their services to actual users affected. There are industries where this might not be such a big burden (e.g. air travel) but in some cases tracking down users might be troubleshooting (e.g. gas storage system operators). As every industry uses specific parameters and criteria to measure the performance of their services, and some of them don't have end users that can be measured, the approach taken at MS level might go beyond the three parameters proposed by the Directive.

Each MS may decide also on industry specific parameters and thresholds, to reflect the reality within a sector or national particularities (e.g. different thresholds in the quality of service apply to electricity transmission operators on North EU and South EU), when measuring the significance of incidents.

The sectoral annexes (A) provide a good input on this matter. ENISA has tried, as much as possible, to include industry specific best practices within this guideline.

Taking into account the remarks above, we can define several methods of measuring incident significance. It is in our understanding that in order to determine significance we must rely on a certain set of indicators based on measureable parameters and well defined thresholds.

In terms of **parameters** to be used the following approaches can be taken:

1. **Use the 3 parameters approach - plain straightforward approach fully aligned with NISD requirements**

Significance can be measured using only the 3 parameters mentioned above. In this respect every operator should carefully collect this type of data when affected by an incident. A generic threshold can be set at national level (e.g. 1 mil. Users affected), or different thresholds per industry (e.g. health: 100.000 patients affected, energy: 1 mil. users affected).

2. **Use an extended generic set of parameters, besides the ones imposed by the NISD**

MS can also choose to use more parameters when determining significance. This document provides some insights on extra parameters that can be used if we wish to make the process more rigorous (e.g. socio-economic impact, market share etc.). The thresholds can be applied generic (same level for all industries) or sector based (different levels per sector).

3. **Use sectoral sets of parameters, adapted to particularities within each sector/subsector**

MS can also choose to adopt sector specific parameters besides the 3 mandatory ones. In this respect the result will be sectoral incident notification policies based on different parameters and thresholds.

In terms of **thresholds** the following approaches can be applied:

1. **Generic thresholds for all sectors/subsectors**

MS can choose to set a generic threshold policy for all sectors (e.g. 1 mil. Users affected no matter what the industry). This approach will be insensitive to sectoral particularities.

2. **Subsector based thresholds**

Whether going for a generic or sectoral based approach in terms of parameters, MS can choose to apply sector based thresholds, meaning that one sector can have different thresholds than others. This approach is expected to be closer to the real risk level within each sector.

3. No thresholds policy – all incidents reported on all OES

Within our analysis we have also identified approaches where MS will apply a policy where all incidents will be notified, if the operator has been identified as essential. This is a good approach in case national authorities in charge want to be aware of all types of incidents affecting the sectors.

Below you will find a table summarizing the approaches stated above.

Thresholds / Parameters	Generic thresholds	Sector/Subsector based thresholds	No thresholds
NISD 3 parameters approach	All incidents in all sectors above the generic thresholds are reported.	Incidents are reported in a sector/subsector if the particular thresholds are met.	All incidents in all sectors are reported as long as the operator is identified as essential.
Extended set of generic parameters	All incidents in all sectors above the generic thresholds are reported.	Incidents are reported in a sector/subsector if the particular thresholds are met.	All incidents in all sectors are reported as long as the operator is identified as essential.
Sectoral sets of parameters	-	Incidents in any sector are reported if the thresholds of that particular sector are met.	All incidents in all sectors are reported as long as the operator is identified as essential, and based on the sector's specific parameters.

Tab. 1 – Determining substantial incidents

2.5 Requirements regarding cross border collaboration in case of incidents

Art. 8 (4) mentions that "The single point of contact shall exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group".

Art. 14 (3) mentions that "Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident."

Also art. 12 (3)(f) (IV) refers to the fact that the CSIRTS Network can discuss, explore, identify "principles and modalities for coordination, when Member States respond to cross-border risks and incidents".

Art. 11 (3) (l) mandates CG to support, with ENISA's assistance, the exchange of best practices in relation to cross-border dependencies, regarding risks and incidents.

Although there is a clear emphasis on the importance of cross border incidents and the sharing of information in such situations, the NISD does not describe a clear approach to be taken and leaves room for further development in the area. To fulfill the requirements mentioned above, further development must be done in the future to elaborate on possible approaches and guidelines.

Nevertheless, some important key factors have to be taken into account when developing cross-border incidents response policies:

- In case of cross border impact information has to be sent to affected stakeholders as soon as possible. Any delays might seriously impact the stakeholders that are affected but don't have a mean of controlling the root cause.
- A clear and comprehensive procedure must be put in place, so that all parties involved are aware of the steps to be taken and responsibilities.
- Having common formats and procedures for sharing information is crucial; a standardized approach of sending/receiving data is desirable so as to improve the efficiency and speed of the exchange. Also, the use of a tool/tools is highly recommended.
- A coordinator must be put in place for any event, in order to oversee the process and make sure that the responsible parties are providing the necessary data.

2.6 OES relying on other services

Art. 16 (5) mentions that "*Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator.*" Consequently, it is the responsibility of the OES, and not of the DSP, to notify the incident to the competent authority.

3 Parameters used to measure impact of incidents

In order to ensure a high common level of network and information security across all the EU Member States, the NISD introduces mandatory incident notification obligations, amongst several other requirements. To this end, mainly art. 14 (3) indicates that "operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide". An exact definition of a significant impact of an incident was not included in the approved version of the NISD, however a definite list of parameters that must be taken into account when ***determining the impact of incidents*** are prescribed as follows:

(a) the number of users affected by the disruption of the essential service;
(b) the duration of the incident;
(c) the geographical spread (area affected by the incident);

Additional parameters can also be taken into account by MS. Such a list of relevant parameters might be completed by the provisions of art. 6 (1), referring to factors to be used when ***determining the significance of a disruptive effect***. The provisions of art. 6 are mostly relevant in connection to the identification of OES, providing some factors to be taken into account when identifying if an operator provides essential services or not. In this respect we can conclude that MS have at their disposal also the list of parameters below:

(d) the dependency of other OES sectors on the service provided by the affected entity;
(e) the impact that incidents have, in terms of degree and duration, on economic and societal activities or public safety;
(f) the market share of that entity;
(g) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

A survey has been launched for both public and private stakeholders, in order to collect feedback.

3.1 Number of users affected by the disruption

Users = the number of affected natural persons and legal entities with whom a contract for the provision of the service has been concluded.

The number of users has been indicated as being used by more than 75% of the respondents to the survey, suggesting that we can consider it one of the main indicators to be used when determining the significance of incidents.

Although the definition might sound clear enough there are certain particularities per industry type. It might be easy to determine the number of users in sectors related to Energy, Transport or Finance due to the straightforward business model that they use and the particularities of the physical ways of delivering their services (pipes, cables etc.) but there are other sectors where the situation might be challenging. For example, in the HEALTH sector the number of users might be considered the number of patients that are treated within the affected clinic/hospital during the time of the incident. But we might also have the case where new persons (possible patients) are affected, that were not registered as patients before the incident starting point. Hospitals usually serve geographical areas (especially in case of emergencies) and the number of population within that region might be also taken into account when determining the number of users. Other particularities might emerge for the digital infrastructure sector (DNS, IXPs, ccTLD).

Another challenge in this area might be the lack of visibility of the operators as regards the actual number of users affected. Usually operators from all sectors see only the first layer of affected users, meaning the ones with whom they have a direct connection (clients, households etc.). A second layer of users might also be affected in case some users are also providing services based on the particular service that was affected (e.g. dependency on energy). In this case, we must point out that the approach to measure the number of users affected by an incident should be simple and pragmatic, so that OES can comply. Asking them to provide information that they cannot obtain or for which they should make considerable efforts is not desirable.

3.2 Duration of the incident

Duration of an incident (NIS downtime) = the period of time when an essential service offered by a OES is unavailable due to an impairment affecting the confidentiality, integrity, availability or authenticity of the underlying computer system that supports the provision of the service.

Duration (time interval) is a parameter considered of utmost importance and used by all of the respondents (75%). All respondents that indicated the use of "number of users" parameter selected also "duration of an incident". This indicates the use of both parameters, probably together. Nonetheless, even for this arguably basic parameter, the survey responses revealed differing practical approaches as to what regards measuring duration and the diverse thresholds applied.

For instance, depending on the incident type, the timer might start from the identification of the breach, or from the service degradation notice. Finalizing the incident might be considered the time where all services have been fully recovered (time to recover) or the time when the systems were fully disinfected (in case of malware infections). In the context of the NISD, since the focus is on the continuity of the service, the duration of the incident should be measured (and consequently reported) as starting from the moment when the provision of the service was affected up until the time of full recovery. Other timings related to the underlying network and information system itself can also be taken into account (e.g. the time of the discovery of the root cause, the time for the full recovery of the service) but the duration of the significant incident has to be considered as the period of time when the essential service was not provided properly.

When considering the duration of an incident we have to take into account others parameters also, such as the number of users affected. Duration cannot be used only by itself when determining significance, as it will not be relevant without any other parameter. We might have situations where although the duration might be a high value, the affected users are not so many, or the other way around. The combination with the USERTIME indicator, might help achieving better flexibility when covering real life scenarios (very long incidents with few users affected or very short incidents with many users affected).

3.3 Geographical spread

Geographical spread = Member States or regions within EU where users were affected by impairments of the essential service affected.

35% of the respondents indicated using the geographical spread as a parameter when measuring the impact of incidents. Mainly respondents come from traditional industries like Transport, Energy, Banking and Healthcare. Obviously the business model of these industries depends a lot on reaching out to as many geographical areas as possible. In their cases identifying the geographical area affected by an incident is not difficult, more than that the whole incident response/recovery processes are based first on the identification of the geographical areas affected.

There are also sectors where the geographical spread might not be such an important parameter. Digital infrastructure operators do use "geographical area affected" as an established parameter to measure impact

of incidents, but not necessarily in the conventional political way we think of, meaning identifying regions or countries. The intense use of web related technologies has made this task exceedingly difficult. Although Internet fragmentation is a fact nowadays, whether from technical, commercial or political standpoints, this is not necessarily embraced by Digital operators unless there is a business need in this sense. Especially DNS services might not serve users based on geographical borders, as one DNS server located in EU (or outside) might receive requests from different geographical area. Nevertheless, there are DNS services out there that are used mainly within certain geographical areas.

Therefore, a simple approach for defining the geographical spread, which can be applied by multiple types of operators, is a must in this case. Consequently, a scale of detailing can be applied, starting from a bottom level where only a yes/no answer can be submitted if the incident has affected EU regions, and ending with a top detailed level where countries and regions can be specified, if known.

Possible units of measure for geographical spread: regions within a country, % of the total area, number of cities/municipalities affected, km^2 affected, number of countries affected, continents affected, etc.

Reporting geographical spread has to be adapted to specificities within the sectors. For sectors where this parameter is crucial, a proper and relevant way of reporting must be put in place. But, for sectors (especially digital) where the services offered might not have geographical constraints a suitable method of reporting has to be considered.

3.4 Dependence of other OES sectors on the service provided by the affected entity

Dependence of other sectors = one-directional reliance of an asset, system, network, or collection thereof – within or across sectors – on an input, interaction, or other requirement from other sources in order to function properly[2]. (In the context of the NISD we might interpret it as the level of reliance of other OES on an essential service provided by one OES.)

30% declared taking this parameter into account when determining the significance of incidents. Most of the answers come from respondents within the Transport sector and some from Banking and Healthcare.

OES systems can span large geographical areas and be located in multiple remote field sites that can be interconnected to one or several central locations, which at the same time may also be sharing communication data amongst each other and other operational sites. OES are dependent on communication infrastructures, energy and other necessary resources and in many cases these are not under the control of the same organization. For example, the dependencies of Industrial Controls Systems (ICS) on the underlying ICT communication infrastructure are just one example of the multiple interdependencies that can arise when addressing critical infrastructures. ENISA's document "Communication network dependencies for ICS/SCADA Systems", published January 2017, provides a good overview in this area.

[2] U.S. Department of Homeland Security, 'National Infrastructure Protection Plan' (2009). <http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf>

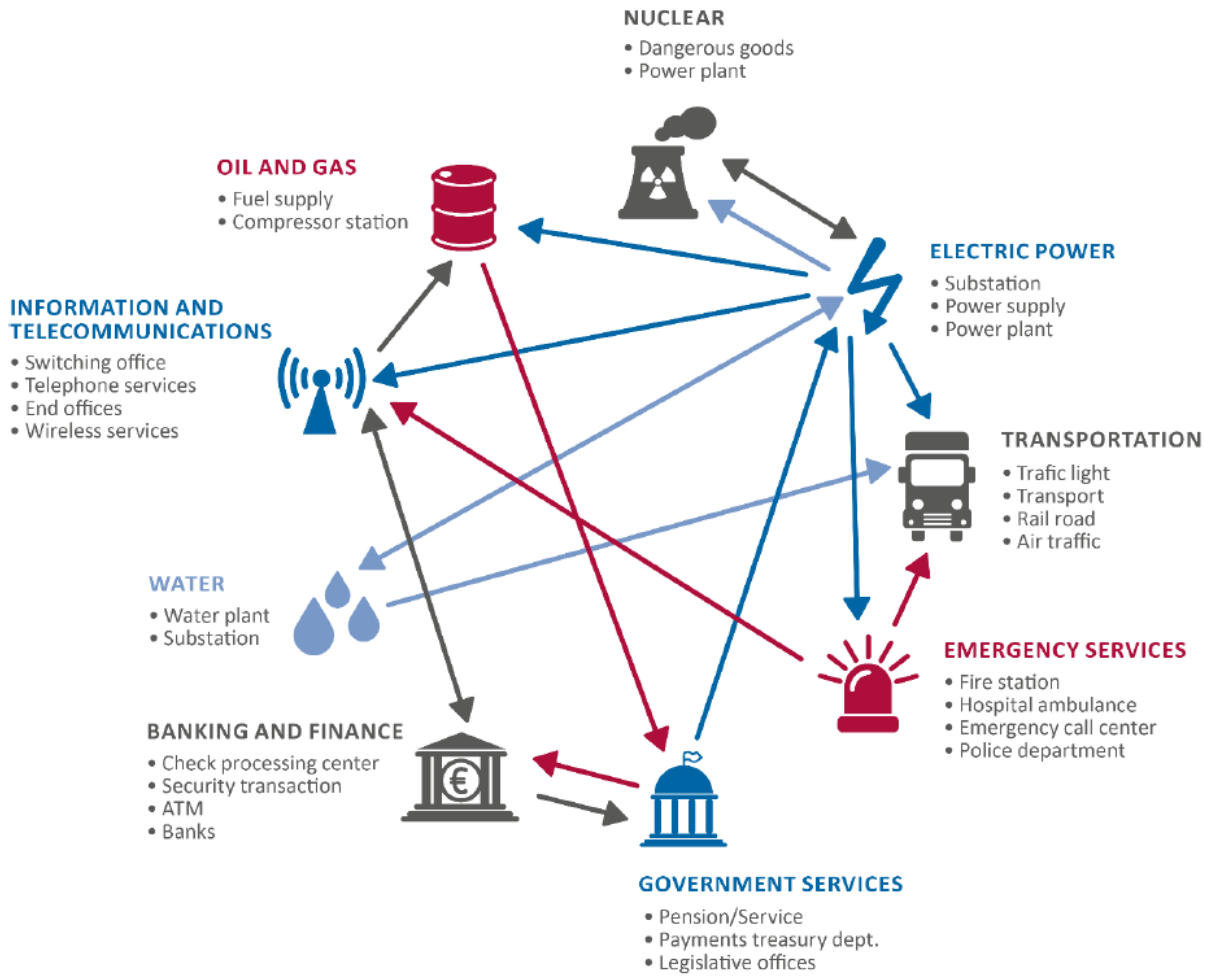

Fig. 2 – Concept of interdependencies in Critical Infrastructure[3]

Knowing the dependencies on a particular OES is a useful parameter as it will help in better understanding the overall impact of a particular incident. An energy blackout within a certain geographical area can also affect hospitals, transport, financial systems and others. In this respect it might be more useful if the "dependency of other sectors" is assumed as "dependency of operators on a particular OES". Considering from a generic point of view we are all aware that Finance (and basically any other sector) is dependent on Energy but, if a particular power plant goes down is better to be aware about which other essential operators are affected by the blackout within the same geographical area.

But in order to identify the interdependencies affected by a certain incident one must have an overview of those above. There are several ways of doing this:

1. **Identifying interdependencies during the identification process:** According to Art. 5 (1) of the NISD Member States "shall identify the operators of essential services with an establishment on their territory". This implies that Member States will have a full list of operators permanently updated. At this point national authorities can identify all interdependencies by requiring the OES to declare them during the identification process.
2. **Affected interdependencies reported during the incident notification process:** This option implies that the OES that is affected by an incident will also report the interdependencies affected that it is aware of. In this case the OES must be aware of all other OES that rely on him. This requirement can

[3] https://www.enisa.europa.eu/publications/ics-scada-dependencies

be solved by imposing some kind of notification requirement within the commercial contracts signed between OES. In this way all OES are aware of each other and can better communicate in case of incidents.

3. **Correlation done by national authorities based on multiple incident notifications:** Multiple OES can submit notification reports that have the same root cause. National authorities responsible for receiving the notifications can correlate the data received and identify interdependencies affected. This option might require more effort within a short (and maybe critical) period of time.

We acknowledge the difficulty of applying such parameter in the incident notification process, but we also consider that is something worthwhile taking into account, especially when developing national incident response procedures.

3.5 The impact on economic and societal activities or public safety

Extent of the impact on economic and societal activities = The detrimental effects of an incident on the activities of users, that generate either economic or social damages or affect the public safety.

58% percent of the respondents to our survey have declared using this parameter when determining the impact of an incident.

In most of reported cases, the measurement unit was related to the internal resources lost or spent for fixing the problem. Most operators are focusing on identifying the impact on their own organization. Nevertheless, in the context of the NISD, by impact on economic and societal activities we refer to possible damages brought to the functioning of the EU internal market. Individual economic impact on a single OES might not be sufficient in this context. The sum of individual impacts suffered by each of the affected users might be a response in this case, but this type of information could be unknown to the OES. Generally, OES have visibility only on the first layer of affected users, the ones that have actually made an agreement with the OES.

Public safety (protection of citizens, organizations, and institutions against threats to their well-being – and to the prosperity of their communities) is also another unknown area for OES. Although in some cases (Energy, Transport) the impact might be known on a relative scale, the real impact can only be measured and communicated by a national authority. Public safety/security usually in the responsibility of the government and might be difficult for OES to determine this kind of impact.

Asking the OES to collect all this data is probably unreasonable and could require plenty of additional resources and could ultimately prove impossible to do. In conclusion, measuring the real impact on economic and societal activities requires many resources and has high probability of failing due to inconsistent or incomplete data.

A simple yet straightforward approach of measuring the indicator can be based on the recorded effects onto predefined thresholds of users. Absolute thresholds (e.g. 1 mil users.) or relative thresholds (percentages of population) could therefore be used. This can be used in connection with other parameters: number of users and duration.

3.6 The market shares of the OES

Market share= the percentage of a market (defined in terms of either units or revenue) accounted for by a specific entity.

Only 7.5% of the respondents declared using market share when measuring the impact of incidents. All of them were public authorities. No further details were given as with regard how this parameter is used.

Market share gives a good overview of the importance of an operator on a specific market. Knowing the market share might help in identifying possible significant incidents and the extent of their impact. The bigger the market share, the bigger the impact in case of an incident. It is also an important indicator in identifying essential operators at Member State level. However, the market share is not always measurable and known, as some operators are not making this figure available.

When using market share public authorities have to be sure that they can collect such data and preserve its confidentiality. In more regulated industries (energy, finance, transport) the market share might be easy to find out as reporting certain figures regarding their activities is mandatory.

When measuring market share it is important to use units of measure that are relevant in the context of the impact that an incident can produce. Taking into account the revenue might not be a good option as it will not properly indicate the real impact on the public. In this respect using other units of measure such as number of users or percentage of the total units within a market (e.g. delivered MWh out of total, passengers transported, throughput Gbit/sec etc.) might be a more suitable option. As mentioned before market share should not be directly reportable as part of a notification, but something that is known by the authority a priori so that the real impact of the incident can be properly determined.

3.7 Availability of alternative means for the provision of the affected service

The indicator is about the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service. A quick example in this case would be the use of an alternative DNS server if the main one goes down.

Alternative means for the provision of the service might come from inside the OES (the use of another transport mean, another equipment, another energy supplier etc.) or from outside, by using another OES. It is worthwhile mentioning that when alternative means of provision are available (especially within the operator), incidents might not classify as significant in the end.

In particular cases alternative means of providing the service are not available (e.g. isolated geographical area etc.) turning most of the incidents into significant ones, especially in cases where the service is of basic need for the population (e.g. energy).

This parameter has to be taken into account in the identification process. Nevertheless, it can also be taken into account when developing incident response procedures and regulations. Alternative means of providing the service should exist within the operator as long as this is possible, and cooperation between operators in this area must be encouraged if the authority considers the necessity. Significant impact upon the population should be avoided with any means available, alternative means of transportation being one of them.

4 Conclusions

The current study has uncovered some concerns that must be addressed while implementing the OES incident reporting provisions of the NISD. The multitude of sectoral approaches mirrored the numerous discrepancies between types of OESs and the corresponding business models adopted, thus creating a deep pool of sometimes incompatible variables that must be taken into account when approaching such a regulation. For example, a simple parameter imposed by the Directive, such as “number of users”, can mean different things to different types of providers, from simple clients of an electricity provider to potential patients of a hospital.

Achieving convergence between the myriad of existing approaches while sticking to the formal requirements might be troublesome. Nevertheless, the EU’s first OES incident notification requirements as part of the first EU wide set of rules on cyber-security are a major step forward towards achieving a common level of resilience across the Union. In a perpetually fluctuating technological landscape that affects our livelihoods while having increasing economic and societal impact as a whole, a first step, in understanding the real threats and vulnerabilities that we have to confront, has been taken through the adoption of the NISD along with its two main requirements: mandatory incident notification and minimum security measures. From now on, a “small steps” approach must be applied in implementing the Directive, that has to undergo periodic reviews and updates.

This document provides a preliminary guideline on how incident notification provisions for OES could be effectively implemented across EU. Based on valuable input from Member States and companies directly impacted by the Directive, this guideline arises from their good practices in matters such as identifying types of incidents, parameters and thresholds and results in an outline proposal that can support harmonized implementation across EU.