Guidelines on notification of Digital Service Providers incidents

Formats and procedures

CG Publication 06/2018

NIS Cooperation Group

July 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

This document provides non-binding technical guidance for national competent authorities on the mandatory notification requirements in the NIS directive (2016/1148) for DSPs (Article 16), as further specified in the subsequent implementing regulation C(2018)471, for the requirement by the Member State of main establishment (Article 18) to inform other Member States in case of cross-border impact (Article 16), and for the annual summary reporting by single points of contact to the NIS Cooperation Group (Article 10).

This technical guideline was developed under work stream 5 of the NIS Cooperation Group (NIS CG) Work Program 2018-2020, on "Digital Service Providers". Work stream 5 is led by experts from the national competent authority of Ireland, supported by experts from ENISA and involving the European Commission.

1.1 Target audience

This document addresses the national competent authorities and CSIRTs implementing the NIS directive.

1.2 Goal and scope

The goal of this document is to provide non-binding technical guidance to national competent authorities and CSIRTs, with regard to formats and procedures regarding the notifications of incidents by DSP, to facilitate alignment in the implementation of the NIS directive across the EU.

Alignment of the notification templates for incidents is important for:

- **Cross-border collaboration:** Efficient cross-border collaboration between authorities and/or CSIRTs in different EU countries benefits from a common taxonomy and from agreement about a minimum set of information to be included in templates.
- **Aggregation and analysis:** With a common taxonomy and terminology the NIS Cooperation group can aggregate and analyse incidents and identify common root causes in a sector or across the EU. Aggregation also provides a layer of anonymization, which makes it easier to inform the public and the private sector about common root causes or crosscutting issues.

1.3 Versions and changes

This is a living document and will be updated by the NIS Cooperation Group, when necessary, taking into account the experience gained from the ongoing implementation in the Member States.

2 Legal reference

In this section, only for the sake of reference, we quote verbatim the most important parts of the text in the NIS directive and the subsequent implementing regulation explaining thresholds for notification by DSPs.

2.1 Recitals

There are a number of recitals specifically referring to the incident notifications.

> *(32) Competent authorities or the computer security incident response teams ('CSIRTs') should receive notifications of incidents. The single points of contact should not receive directly any notifications of incidents unless they also act as a competent authority or a CSIRT. A competent authority or a CSIRT should however be able to task the single point of contact with forwarding incident notifications to the single points of contact of other affected Member States.*
>
> *(33) To ensure the effective provision of information to the Member States and to the Commission, a summary report should be submitted by the single point of contact to the Cooperation Group, and should be anonymised in order to preserve the confidentiality of the notifications and the identity of operators of essential services and digital service providers, as information on the identity of the notifying entities is not required for the exchange of best practice in the Cooperation Group. The summary report should include information on the number of notifications received, as well as an indication of the nature of the notified incidents, such as the types of security breaches, their seriousness or their duration.*
>
> *(59) Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing. Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats against possible reputational and commercial damage for the operators of essential services and digital service providers reporting incidents. In the implementation of the notification obligations, competent authorities and the CSIRTs should pay particular attention to the need to keep information about product vulnerabilities strictly confidential, prior to the release of appropriate security fixes.*
>
> *(60) Digital service providers should be subject to light-touch and reactive ex post supervisory activities justified by the nature of their services and operations. The competent authority concerned should therefore only take action when provided with evidence, for example by the digital service provider itself, by another competent authority, including a competent authority of another Member State, or by a user of the service, that a digital service provider is not complying with the requirements of this Directive, in particular following the occurrence of an incident. The competent authority should therefore have no general obligation to supervise digital service providers.*
>
> *(64) Jurisdiction in respect of digital service providers should be attributed to the Member State in which the digital service provider concerned has its main establishment in the Union, which in principle corresponds to the place where the provider has its head office in*

the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect. This criterion should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not criteria for determining the main establishment.

(67) Entities falling outside the scope of this Directive may experience incidents having a significant impact on the services they provide. Where those entities consider that it is in the public interest to notify the occurrence of such incidents, they should be able to do so on a voluntary basis. Such notifications should be processed by the competent authority or the CSIRT where such processing does not constitute a disproportionate or undue burden on the Member States concerned.

2.2 Article 16

Article 16 of the NIS Directive, paragraph 3, explains the notification of incidents by Digital Service Providers (DSPs):

Article 16: Security requirements and incident notification

(…)

3. Member States shall ensure that digital service providers notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union. Notifications shall include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact. Notification shall not make the notifying party subject to increased liability.

4. In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account:
(a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services;
(b) the duration of the incident;
(c) the geographical spread with regard to the area affected by the incident;
(d) the extent of the disruption of the functioning of the service;
(e) the extent of the impact on economic and societal activities.
The obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in the first subparagraph.

5. 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.

6. Where appropriate, and in particular if the incident referred to in paragraph 3 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law, or national legislation that complies with Union law, preserve the digital service provider's security and commercial interests as well as the confidentiality of the information provided.

7. After consulting the digital service provider concerned, the competent authority or the CSIRT and, where appropriate, the authorities or the CSIRTs of other Member States concerned may inform the public about individual incidents or require the digital service provider to do so, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest.

8. The Commission shall adopt implementing acts in order to specify further the elements referred to in paragraph 1 and the parameters listed in paragraph 4 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2) by 9 August 2017. [see below]

9. The Commission may adopt implementing acts laying down the formats and procedures applicable to notification requirements. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).

10. Without prejudice to Article 1(6), Member States shall not impose any further security or notification requirements on digital service providers.

11. Chapter V shall not apply to micro- and small enterprises as defined in Commission Recommendation 2003/361/EC (1).

2.3 Implementing regulation

The thresholds for notification are explained in Article 3 and 4 of the Implementing regulation.

Article 3: Parameters to be taken into account to determine whether the impact of an incident is substantial

1. With regard to the number of users affected by an incident, in particular users relying on the service for the provision of their own services referred to in point (a) of Article 16(4) of Directive (EU) 2016/1148, the digital service provider shall be in a position to estimate either of the following:

(a) the number of affected natural and legal persons with whom a contract for the provision of the service has been concluded; or

(b) the number of affected users having used the service based in particular on previous traffic data.

2. The duration of an incident referred to in point (b) of Article 16(4) means the time period from the disruption of the proper provision of the service in terms of availability, authenticity, integrity or confidentiality until the time of recovery.

3. As far as the geographical spread with regard to the area affected by the incident referred to in point (c) of Article 16(4) of Directive (EU) 2016/1148 is concerned, the digital service provider shall be in a position to identify whether the incident affects the provision of its services in specific Member States.

4. The extent of disruption of the functioning of the service referred to in point (d) of Article 16(4) of Directive (EU) 2016/1148 shall be measured as regards one or more of the following characteristics impaired by an incident: the availability, authenticity, integrity or confidentiality of data or related services.

5. With regard to the extent of the impact on economic and societal activities referred to in point (e) of Article 16(4) of Directive (EU) 2016/1148, the digital service provider shall be able to conclude, based on indications such as the nature of his contractual relations with the customer or, where appropriate, the potential number of affected users, whether the incident has caused significant material or non-material losses for the users such as in relation to health, safety or damage to property.

6. For the purpose of paragraph 1, 2, 3, 4 and 5, the digital service providers shall not be required to collect additional information to which they do not have access.

Article 4: Substantial impact of an incident

1. An incident shall be considered as having a substantial impact where at least one of the following situations has taken place:

(a) The service provided by a digital service provider was unavailable for more than 5 000 000 user hours whereby the term user hour refers to the number of affected users in the Union for a duration of sixty minutes;

(b) The incident has resulted in a loss of integrity, authenticity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100 000 users in the Union;

(c) The incident has created a risk to public safety, public security or of loss of life;

(d) The incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1 000 000.

2. Drawing on the best practice collected by the Cooperation Group in the exercise of its tasks under Article 11(3) of Directive (EU) 2016/1148 and on the discussions under point (m) of Article 11(3) thereof, the Commission may review the thresholds laid down in paragraph

2.4 Member State of Main Establishment (Article 18)

Article 18 of the NIS Directive (2016/1148) covers the principle of jurisdiction regarding which Member State competent authority or CSIRT, the digital service provider provides notifications to in respect of substantial impacts on the provision of its digital services in multiple Member States. This provision also covers circumstances where the digital service provider has no establishment in the European Union, in which case

it must designate a representative in a Member State and that Member State then has jurisdiction regarding its digital services in the Union.

> *1. For the purposes of this Directive, a digital service provider shall be deemed to be under the jurisdiction of the Member State in which it has its main establishment. A digital service provider shall be deemed to have its main establishment in a Member State when it has its head office in that Member State.*
>
> *2. A digital service provider that is not established in the Union, but offers services referred to in Annex III within the Union, shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. The digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established.*
>
> *3. The designation of a representative by the digital service provider shall be without prejudice to legal actions which could be initiated against the digital service provider itself.*

2.5 Annual summary reporting to the NIS Cooperation group (Article 10)

Article 10 of the NIS Directive (2016/1148) requires that the single points of contact provide summary reports to the NIS Cooperation Group about the notifications received from OESs and DSPs.

> *By 9 August 2018, and every year thereafter, the single point of contact shall submit a summary report to the Cooperation Group on the notifications received, including the number of notifications and the nature of notified incidents, and the actions taken in accordance with Article 14(3) and (5) and Article 16(3) and (6).*

3 Scope

This section outlines which incidents are in scope of the notification and reporting requirements.

3.1 Services in scope

The digital services in scope are:

- Search engines
- Online marketplaces
- Cloud computing services

Digital service providers are defined in the text of the NIS Directive, Article 4(17), (18), (19), to be read in conjunction with corresponding recitals (15), (16) and (17). Additional information and relevant examples on DSPs within the scope of the Directive can be found in Section 4.4.1. of the Annex to the Communication on 'making most of NIS' issued by the Commission in September 2017[1].

3.2 Incidents in scope of the notification requirements

Incidents in scope are those events, which have an adverse effect on the security of the network and information systems, i.e. the incident has an impact on the availability, authenticity, integrity or confidentiality of the digital service.

Incidents have to be notified when there is a substantial impact on the provisioning of the service. The thresholds are as follows:

- The incident caused an unavailability of the core service more than 5 000 000 user hours.
- The incident caused a loss of confidentiality, integrity or authenticity of data or services affecting more than 100 000 users.
- The incident created risks for public safety, public security or of loss of life
- The incident caused damage to at least one user in the Union where the damage caused to that user exceeds EUR 1 000 000.

Note that, as explained in Recital 10 of the Implementing Regulation, this is a non-exhaustive list of cases of when an incident should be considered as having a substantial impact. As the implementation progresses, the Cooperation Group will evaluate these thresholds with a view to updating this list.

[1] Annex to the Communication from the Commission to the European Parliament and the Council on *Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*. COM(2017) 476 final/2

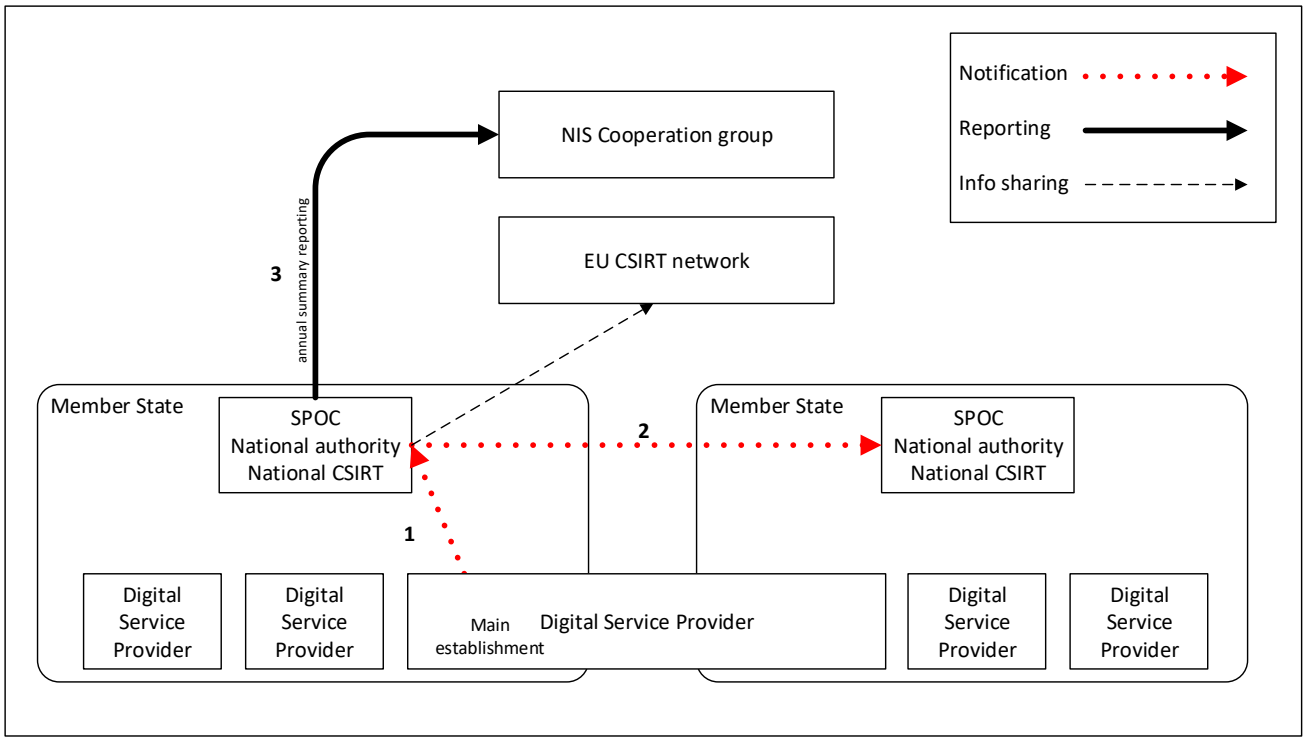
4 Procedures

4.1 Overview and examples

The NIS directive contains three mandatory notification and reporting requirements. The processes are depicted in the diagram below:

1. A DSP must *notify* incidents with *substantial* impact, without undue delay, to the national authority and/or the national CSIRT of the Member State of main establishment.
2. If the notified incident *concerns* two or more EU Member States, then the Single Point of Contact (SPOC) of the Member State of main establishment shall *inform* the SPOC in that other Member State.
3. Annually, the national competent authorities of the Member States of main establishment send an *annual summary report* to the NIS Cooperation group, about the notification received from DSPs.

Besides this, the CSIRTs share information with the EU CSIRT network on a *voluntary basis*. For example, information sharing about Indicators of Compromise (IOCs) between CSIRTs happens continuously, on a daily basis, even when there are no incidents. The voluntary information sharing between national CSIRTs and within the EU CSIRT Network (depicted in the diagram with a black dashed arrow) is out of scope of this document.



Note also that in the diagram, for the sake of simplicity, the three roles (the national authority, the CSIRT, and the Single Point of Contact) are combined in one box. In practice in the different EU Member States, different organizations may play these roles, depending on the national circumstances and setup. For example, in one Member State sectorial authorities may be involved, while in another Member State there may be a central authority hub/centre for crises, which then forwards notifications about cybersecurity incidents to a national CSIRT and/or other relevant national authorities.

Note that there is an important difference with respect to the notification requirements for Operators of Essential Services: A DSP is only required to notify to the competent authority and/or CSIRT of the country where it has its main establishment, even if it has customers in another EU Member States. The competent authority of that EU Member State has jurisdiction (see Article 18 about Jurisdiction and territoriality). This also means that the authority receiving the notification must cooperate with the authorities in EU countries where the incident has an impact.

We give an example of incidents and notification, illustrating the purpose of notification:

Cloud service outage: *A large data centre suffers a major fire and there is a total data centre blackout, affecting thousands of business customers, causing a service disruption for 25 hours. The cloud service provider provides services and has customers in a number of EU Member States. The national authority and the CSIRT of the Member State, where the cloud service provider has its main establishment, receive the notification. There is considerable concern with the customers because of confusing public statements from the provider and confusing news coverage. The national competent authority consults with the cloud provider, and later, in agreement with the cloud provider, issues a public statement reassuring the customers that most customer data will be recoverable, because the provider has off-site backups. The national competent authority of the Member State of main establishment also informs, via its SPOC, the other Member States affected, via their SPOC.*

4.2 Alert and follow-up notifications

Cybersecurity incidents are dynamic and the situation can change rapidly. It may be unclear at first what is the nature of an incident. An outage seemingly caused by a software bug sometimes turns out to have been caused by a cyber-attack, and vice versa. A DDoS (distributed denial-of-service) attack may seem over at first, but new waves can come later, over several days. This means that a one-off, one-way, message to the national competent authority and/or CSIRT is often not enough and follow-up may be needed.

4.2.1 Alert notifications

Immediate alert notification by the provider serves as an alert to the national competent authority and/or the CSIRT to allow them to:

- Offer support to the affected organization, for example, the CSIRT could give technical support[2]
- Assess the potential impact for critical services, citizens, the society, the economy, etc.
- Inform, in exceptional circumstances and when in the public interest, other organizations, so they can take action.
- Prevent spreading or reduce the impact by warning and sharing information with relevant organizations, for example with other DSPs, OESs, CSIRTs, etc.
- Inform authorities abroad when there is substantial impact across the border in another EU Member State.

It is good practice to keep the first alert notification short and simple, following up with more information as it becomes available. In the early stages the organization often does not have all the information.

Note that because the information in the initial alert notification may be incomplete or inaccurate at first it is good practice to verify the received information and to consult with the DSP before taking action.

[2] Note that the NIS Directive does not obligate national authorities or CSIRTs to support affected organization.

4.2.2 Follow-up notifications

When the initial alerting notification happens, the affected organization often does not have the complete picture. The total duration and total impact of an incident is not known until the incident is resolved. The root cause may be unknown initially. The total duration and root cause, for example, are crucial pieces of information for the competent authority to fulfil their supervisory role. It is therefore good practice to follow up the initial alerting notification with more detailed follow-up notification, containing more information about the incident. The timing and rhythm for these follow ups depends on the situation.

Follow-up notifications are used to confirm and update preliminary information and to provide additional information about the incident that has become available. A full report after the incident is resolved, also known as a *post-mortem incident report*, allows the national competent authority and/or CSIRT to:

- Understand the total impact of incidents in terms of total duration, total number of users, total economic and societal impact
- Understand the root causes of incidents, the underlying issues
- Understand if and how similar incidents could be prevented or mitigated in the future

This last step is important for the Member State to evaluate existing policy, to develop new policy initiatives to mitigate incidents, to discuss and address cross-sector issues, etc.

4.3 Incident notification by Digital Service Providers

In this section we focus on the incident notification by the DSP to the national competent authority and/or CSIRT, where the DSP has its main establishment, arrow 1 in the previous diagram.

Timing of notification: Notification about an incident needs to take place as soon as possible**.** Notification typically contains preliminary and limited information. As mentioned already in the previous section, it is good practice to follow up the initial alert notification with more as more information becomes available. The rhythm and timing of these follow-up notifications depends on the setting and the situation.

Notification methods: Member States can offer different methods for receiving notifications about incidents:

- phone call (POTS or IP-based voice/video calls, e.g.)
- plain email,
- email with a form as an attachment (PDF, e.g.),
- online form (HTML over SSL/TLS, e.g.),
- web service API (JSON, XML, e.g.)

Multiple options: It is advisable to point to a preferred method for reporting in order to have a unified approach and develop a manageable routine process for receiving and processing notifications. However It is important to offer several different methods, and to have a fall back, to avoid that an incident notification comes late due to practical issues or technical problems. This is even more important because in the case of an incident certain IT systems may be impaired or unavailable. For example, in the case of a DDoS attack there may be limited internet connectivity preventing the use of an online form, in the case of a computer virus, the office PCs may be unavailable preventing the use of email, in the case of a national crisis, traditional (POTS, 2G) phone networks may be overloaded, preventing phone calls.

Technical and security considerations for different methods: When implementing notification methods it is important to take into account factors like:

- **Confidentiality** – Depending on the nature of the incident and the information in the notification the notifying organization may want to use specific encryption methods to protect confidentiality of the notification. Standard telephone networks and legacy email systems, for example, do not always provide an adequate level of protection.
- **Authenticity of the notification** – It is important, to avoid fake notifications, that a sanity check is done on the received notification, to confirm the information with the affected organization, and to obtain assurance about the information received.
- **Confirmation** – For the notifying organisation it is important to receive a confirmation that the notification was received by the national competent authority and/or CSIRT. It is good practice to include a ticket or case number in the confirmation, allowing the notifying organisation to reference the original notification later on.

We provide some technical and security considerations for the different methods:

- **Phone call:** A phone call is quick to make and does not require internet connectivity. The added advantage of using telephone calls is that with a phone call the notifying organization has a clear confirmation that the notification was received by the national authority and/or CSIRT. It is good to offer also IP-based voice/video calling, via an app for instance, because in certain crises, the legacy telephone system (POTS, 2G) may become overloaded.
- **Email:** Email is widely used in the business world, but it is important to note that email still has major security and reliability issues. There is an increased adoption of email security standards like StartTLS and DMARC, but not all organization support this. Email is not always a reliable method for notification, especially not for the first communication, because emails may be blocked by spam, phishing or security filters. Emails with attachment offer the possibility of using 'offline' forms, i.e. forms that can be compiled offline, by several people in the organization.
- **Email encryption:** As mentioned, there is a growing uptake of StartTLS providing transport layer encryption for the email protocol. Encryption of emails via PGP (often used in the community of cybersecurity professionals) and/or S/MIME is a possibility. It is important to realize that PGP and S/MIME are not always easy to set up and use for people outside the cybersecurity community, requiring some experience and skill, preparation (key-sharing and signing). PGP and doesS/MIME do not always work on all devices. For example, PGP emails may be unreadable on mobile phones, if the user did not set it up or because of interoperability issues. This may be an issue in an urgent crisis situation, when internet connectivity or when access to the usual PCs is disrupted.
- **Online forms:** Online forms can be implemented with open standards (HTML), which means that they work on all platforms and devices, in standard browsers, without special software. Online forms can be implemented using TLS (HTTPS), offering a robust, easy to use, and highly interoperable encryption mechanism. Particularly for ex-post reporting, which is less time-critical and involves more detailed information, using online forms is recommended.

Note that for most of these notification methods there is lack of strong authentication and therefore a risk of spoofing and fake notifications.

4.3.1 Examples of national approaches

Different EU Member States implement the notification requirements differently. For a more detailed discussion about different approaches, we refer to the earlier NIS CG reference document on incident reporting. We give two simple examples for the sake of illustration.

Example A: One-step approach

- *The DSP has to notify the CSIRT, by telephone, as soon as possible.*
- *The CSIRT has a checklist with questions to ask during the call and uses an internal ticketing system to track the incident. The CSIRT confirms receipt of the notification by providing the DSP a ticket/case number.*
- *The CSIRT, which also acts as the SPOC, notifies the SPOCs (national authorities or CSIRTs) abroad when this is necessary.*
- *Depending on the situation, the CSIRT will offer the provider support and/or ask to be kept informed with daily status updates, via email, until the incident is closed.*
- *The national authority can ask the DSP for a full incident report, ex-post, if needed, for example in the case of major incidents.*
- *Every year the national authority discusses together with the CSIRT in order to compile and send the annual summary report to the NIS Cooperation group.*

Example B: Two-step approach

- *The provider has to notify the national authority, as soon as possible, using a short online web form. The form has several checkboxes to indicate the severity of the situation. After submitting the form the DSP receives a ticket/case number, confirming that the notification was processed properly.*
- *The national authority forwards the notification to the CSIRT alerting them that that there is a situation where there support might be needed. The national authority, which acts as the SPOC, also notifies SPOCs abroad if needed.*
- *The CSIRT assesses the situation and engages with the provider asking if support is needed in handling the incident. The CSIRT identifies useful threat information for sharing with peers and/or constituents.*
- *Ex-post, after the incident is resolved, the provider has to send a complete incident report to the national authority, a longer, more complete, online form. This has to be done within 3 weeks. A part of this report is used for annual summary reporting to the NIS Cooperation group.*
- *Every year the national authority uses these reports to publish a full overview of common root causes, total number of incidents, their nature, their impact, etc.*

4.4 Informing other Member States in case of cross-border impact

If a Member State receives a notification about an incident from a DSP, and it is therefore the Member State where the DSP has its main establishment, then the single point of contact (SPOC) of that Member State should inform the SPOCs in the other EU Member States of concern.

Purpose: The purpose is to provide information relevant for the supervision activities of national authorities and/or CSIRTs when implementing Article 16. The other Member States have a right to provide information to the authority that is competent to provide ex-post supervision of the incident in the Member State of main establishment.

Note that the goal of this cross-border notification mechanism is supervision and it should not be relied on as an 'early-warning' mechanism, because it follows a *mandatory* notification, which may come sometime after the incident has started[3].

Procedure and format: This guideline does not propose a detailed procedure or template for the information exchange between Member States about cross-border impact. The timing and content of this bilateral information exchange depends on the situation. Often in the initial phase of an incident not all information is accurate or available. Member States could use the incident notification template (see Section 5) as the basis for sharing information with a SPOC in another EU Member States, but depending on the situation, not all fields and not all the information may be necessary. In some settings information may need to be added, to provide missing context or to inform the other SPOCs about actions being taken by the authority.

Methods: The Commission collects the contact information of the SPOCs in the Member States. The SPOCs in the Member States should use this contact list for cross-border reporting. In the contact list Member States should specify how their SPOC can be contacted, for example via email or telephone.

Confidentiality and need to know: When informing another Member State about an incident with cross-border impact, the single point of contact (SPOC) should take due care to protect the security and commercial interests of the affected organization, when sharing information about an incident. The information included in cross-border notification should allow authorities in MS to make an assessment of the situation and help with decision-making. It should not unnecessarily impact the (commercial) interests of the organization affected by the incident.

Sensitive information and marking: Some information about network and information security incidents could be sensitive. It is important to preserve the security and commercial interests of the affected organization, as well as the confidentiality of the information provided in its notification. The sender of the information, the SPOC informing other Member States, should explain clearly how this information is to be handled by the receiving SPOC and which parts can be shared. Markings, labels, and handling instructions, like for instance the Traffic Light Protocol, could be used for this[4].

Sharing personal data: In general sharing of information should be done in line with the data protection principles included in the General Data Protection Regulation (such as limitation, minimal data use, data security and accountability). If incident notifications contains personal data, then it should be processed only to the extent strictly necessary.

4.5 Annual summary reporting

Annually each Member State should submit a summary report to the NIS Cooperation Group, about the incidents notified by DSPs. To avoid double reporting of incidents, this summary report should regard only the incident notifications received by the relevant authority in the Member State of main establishment. This annual summary report should contain the number of notifications, the nature of the incidents, and the actions taken to comply with the requirements of Article 16(4) and 16(6), i.e. whether or not there was cross-border impact and if authorities and/or CSIRTs abroad were notified.

Purpose: The purpose of annual summary reporting to the NIS Cooperation group is to:

[3] Voluntary sharing of information and early warning is addressed in Article 12 of the NIS Directive about the CSIRT Network and Annex I of the NIS Directive, specifying requirements and tasks of CSIRTs.
[4] https://en.wikipedia.org/wiki/Traffic_Light_Protocol

- To create an EU wide aggregation of notified cybersecurity incidents
- To identify trends, patterns in cyber security
- To inform a more strategic view on cyber security incidents.
- To understand the efficiency and effectiveness of the incident notification requirements and the collaboration and information sharing mechanisms.

This allows the NIS Cooperation Group, the Commission, and Member States in turn, to change existing policy, to develop new policy, to initiate PPPs for specific issues, or to develop additional guidance for national authorities, such as sectorial baselines.

Procedure and format: The detailed procedure for annual summary reporting to the NIS Cooperation Group will be developed and agreed by the NIS Cooperation Group. The template describing the kind of information that should be included in the annual summary reporting is described in Section 5.

4.6 Informing the general public

The competent authority or the CSIRT may need to inform the general public, to mitigate the impact of the incident. The focus of the communication should be on the impact of the incident, for example the impact on the essential services, or the impact on economy/society. Practically speaking, it is often the best and the easiest if the operator itself reaches out to its customers, or the public in general, because it has appropriate channels for such communications, for example a customer website, a helpdesk, etc. However, there may be situations when the authority or CSIRT has to inform the public:

- If public awareness is needed to mitigate the impact of ongoing or future incidents.
- If people outside the current customer base are impacted.
- If the current customer base is very different from the customers originally affected by the incident.
- If the operator is no longer able to inform the public, e.g. when the company ceased operating.
- If the operator did not properly, or will not, inform the public, but there is a critical need to do so.

It is important that before informing the public about an incident, there is a consultation with the organization affected by the incident, the national CSIRT and, if relevant, the CSIRTs and/or competent authorities of other Member States involved, to avoid jeopardizing ongoing incident response efforts, to avoid hampering ongoing investigations, and to avoid unnecessary impact on the security or commercial interests of the organization affected by the incident.

5 Formats

This section includes two templates: One for the national incident notification procedure and one for annual summary reporting.

5.1 Template for incident notification

This section proposes a basic template for incident notifications. and annual summary reporting to the NIS CG. This is intended as non-binding guidance for national authorities in the Member States who are developing and implementing national notification processes, for example in a specific sector. The proposed template comprises information that, if included in national notifications, would allow for a more rapid sharing of information between competent authorities/CSIRTs in cases where an incident has a cross-border impact. Commonly agreed type of information could enhance situational awareness at Member State level (in particular for competent authorities/CSIRTs receiving reports from other Member States) and ensure a swifter follow-up. Moreover, information concerning the nature incident and their impact must be submitted by the Single Point of Contact to the NIS Cooperation Group as part of annual summary reporting.

The parameters[5] to be taken into account to determine whether the impact of an incident is substantial are specified in Article 3 of the Implementing Regulation (EU) 2018/151 on Digital Service Providers[6].

- Nature of the incident
  - Type of threat or root cause that caused the incident, the general category (see Annex A).
  - Severity of the threat, for example using a scale.
  - Description of detailed causes and/or threats (e.g. storm, software bug, ransomware attack, DDoS attack, vandalism, intrusion, etc).
- Impact of the incident
  - Service(s) affected
  - Extent of the disruption (authenticity, integrity, availability, confidentiality) x (data, services)
  - Scale of the impact on society and economy (see Annex A)
  - Geographic spread inside or outside the country
  - Nature of the customers or contracts
  - Risks for health or safety or possible loss of life
  - Damage to property and/or financial losses (euros)
  - Number of users impacted (see Annex A)
  - Duration (see Annex A)
- Contact information
  - Name of the organization affected
  - Contact point for the incident (name, role, contact details, availability)
  - Other parties that may be involved in the incident (e.g. cyber security companies or LEA)
- Operational information

[5] These include the number of users, the duration of the incident, the extent of disruption, the geographical spread, and the impact on economic and societal activities.

[6] Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact

  - Time of incident (start of incident or discovery of incident)
  - Status of incident (ongoing, resolved, under control)
  - Incident details (malware used, inside/outside actor, relation to known campaigns)
  - Expected time to resolve the incident
  - Actions taken or ongoing to mitigate the incident
  - Support requested from the national CSIRT
- Information sharing
  - IT assets affected by the threat (software versions, hardware models, etc).
  - Information about the threat (IoCs, e.g.)
- Ex-post information sharing
  - Actions taken to mitigate the incident
  - Lessons learned

5.2 Template for annual summary reporting to the NIS CG

This section provides guidance with regard to the information that the Single Point of Contact is required to submit to the Cooperation Group every year (starting from 9 August 2018). Categories used for this template (i.e. number of notifications, nature of notified incidents and actions taken in accordance cross-border sharing of information) reflect the Directive's provisions in Article 10(3). In addition, the template includes sub-categories that could be included with a view to adding consistency to the information received by the Group and allowing for a more effective analysis of incident notification across the EU.

The proposed template for the annual summary report for notified DSP incidents is as follows:

- Descriptive information, per Member State:
  - Total number of notifications received
  - General summary, general trends, noteworthy case(s)
- Statistical information, per incident notified, about nature and impact :
  - Type of service impacted by the incident
    - Online marketplaces
    - Search engines
    - Cloud computing services
  - Nature of the incident, indicating one of the root cause categories
    - System failures (e.g. software bug, flawed procedure, hardware failure, etc.)
    - Natural disasters (e.g. storm, earthquake, etc.)
    - Human errors (e.g. mistake, negligence, etc.)
    - Malicious actions (e.g. cyber-attack, vandalism, theft, etc)
    - 3rd party failures (e.g. power cut, internet outage, etc)
  - Impact of the incident, indicating
    - Number of users affected
    - Duration of unavailability
    - Impact on authenticity, integrity or confidentiality of data or service
    - Risks for society or economy
    - Material damage (in euros)
  - If other Member States were concerned and informed

Annex A: Fields used in the templates

In this annex we define and describe some of the fields used in the templates in Section 5.

5.2.1 Citizens affected

Estimate based on a) number of natural and legal persons with whom a contract for the service has been concluded, or b) number of affected users based on past usage data.

5.2.2 Duration

Duration of the impact, i.e. time from the moment the impact of the incident is substantial until the moment the impact is no longer substantial.

5.2.3 Rootcause category

Root cause categories are

- System failures (e.g. software bug, flawed procedure, hardware failure, etc.)
- Natural disasters (e.g. storm, earthquake, etc.)
- Human errors (e.g. mistake, negligence, etc.)
- Malicious actions (e.g. cyber-attack, vandalism, theft, etc)
- 3rd party failures (e.g. power cut, internet outage, etc)

5.2.4 Impact severity scale

- Red - very large impact
- Yellow – large impact
- Green – minor impact
- White - no impact