Guidelines on notification of Operators of Essential Services incidents

Formats and procedures

CG Publication 05/2018

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 and/or the CSIRTs on the mandatory notification requirements in the NIS directive (2016/1148) for OESs (Article 14), for the requirement to inform other Member States in case of cross-border impact (Article 14), for the annual summary reporting by single points of contact to the NIS Cooperation Group (Article 10), and for the voluntary notifications (Article 20).

This technical guideline was developed under work stream 3 of the NIS Cooperation Group (NIS CG) Work Programme 2018-2020, on "Notification Requirements for Operators of Essential Services". Work stream 3 is led by experts from the national competent authority of the Netherlands and Poland, and is supported by the experts from ENISA and involves the European Commission.

This guideline covers two items in the NIS CG Work Programme 2018-2020: 1) "Guidelines on format and procedure of national notifications" (led by the Netherlands) and 2) "Guidelines on the procedure of mandatory sharing of information between affected Member States" (led by Poland). Considering that the above-mentioned items are closely related, the output of both activities are merged into one document.

This is a follow up on the NIS CG Reference document on incident reporting, developed earlier by the NIS CG and ENISA, which gives a detailed overview of different national approaches and perspectives on notification.

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) guidance to national competent authorities and CSIRTs with regard to formats and procedures for the notification of incidents by OES, to facilitate alignment in the implementation of the NIS Directive across the EU.

Alignment of notification processes for OES 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 an agreement about a minimum set of information to be included in national templates.
- **Aggregation and analysis:** With a common taxonomy and terminology the NIS Cooperation Group could aggregate information and identify common root causes in a sector or across the EU. Aggregation also provides a layer of anonymization when speaking about incidents.
- **Efficiency and administrative burden:** Operators of Essential Services often operate in several EU countries. Guidance on notification templates helps MS with aligning the notification templates used in different national incident notification processes.

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 of the NIS Directive 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.

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.*
>
> *(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 14

Article 14 of the NIS Directive explains the notification of incidents by Operators of Essential Services (OESs):

> ***Article 14: Security requirements and incident notification***
>
> *(…)*
>
> *3. 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. Notification shall not make the notifying party subject to increased liability.*
>
> *4. 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.*
>
> *5. On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT 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. In so doing, the competent authority or the CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification.*
>
> *Where the circumstances allow, the competent authority or the CSIRT shall provide the notifying operator of essential services with relevant information regarding the follow-up of its notification, such as information that could support the effective incident handling.*
>
> *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.*
>
> *6. 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.*
>
> *7. Competent authorities acting together within the Cooperation Group may develop and adopt guidelines concerning the circumstances in which operators of essential services are required to notify incidents, including on the parameters to determine the significance of the impact of an incident as referred to in paragraph 4.*

2.3 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).

2.4 Voluntary notification (Article 20)

Article 20 requires MS to process also voluntary notifications about significant incidents from organizations, who are not OES or DSP.

Article 20: Voluntary notification

1. Without prejudice to Article 3, entities which have not been identified as operators of essential services and are not digital service providers may notify, on a voluntary basis, incidents having a significant impact on the continuity of the services which they provide.

2. When processing notifications, Member States shall act in accordance with the procedure set out in Article 14. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary notifications shall only be processed where such processing does not constitute a disproportionate or undue burden on Member States concerned.

Voluntary notification shall not result in the imposition upon the notifying entity of any obligations to which it would not have been subject had it not given that notification

3 Scope

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

3.1 Services in scope

The services in scope are the essential services provided by entities[1] operating in the sectors and sub-sectors listed in Annex II of the Directive, namely:

- Electricity
- Oil
- Gas
- Air transport
- Rail transport
- Water transport
- Road transport
- Banking
- Financial market infrastructures
- Health care
- Drinking water supply and distribution
- Digital Infrastructure

Since the NIS Directive (2016/1148) is a minimum harmonisation legislation, Member States can include other sectors and subsectors and identify entities as OES for essential services in these additional sectors and subsectors.

3.2 Incidents in scope of the notification requirements

Incidents in scope of notification are those incidents, which have an adverse effect on the security of the network and information systems, used for the provision of the essential services, causing a significant disruption of essential services offered by an operator.

The definition of significance can differ between Member States. Whether or not an incident is significant, nationally, depends on the sector, the type of essential service, national circumstances, etc.

The NIS CG, together with ENISA, developed a reference document, which gives an overview of the different national approaches to defining significance, thresholds, etc[2].

[1] Member States are tasked with identifying OES by 9 November 2018. The NIS Cooperation Group's Work Stream 1 has already provided guidance on the identification process of the OES through the reference document "Identification of Operators of Essential Services - *Sharing of good practice related to the criteria defining the criticality of an operator pursuant to art. 5(2) of the directive by means of guidelines*".

[2] The NIS Cooperation Group Reference document on incident reporting for OES incidents includes more details about circumstances in which incidents have to be reported according to the NIS Directive (2016/1148).

4 Procedures

4.1 Overview and examples

The NIS Directive (2016/1148) contains three mandatory notification and reporting requirements. The processes are depicted in the diagram below:

1. An OES must *notify* incidents with *significant* impact, without undue delay, to the competent authority and/or the national CSIRT.
2. If an incident has a significant impact in another EU Member State, then the Single Point of Contact (SPOC) *informs* the SPOC in that other Member State.
3. Annually, the national competent authorities send an *annual summary report*, to the NIS Cooperation Group, about the notification received from OESs.

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 may happen 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.

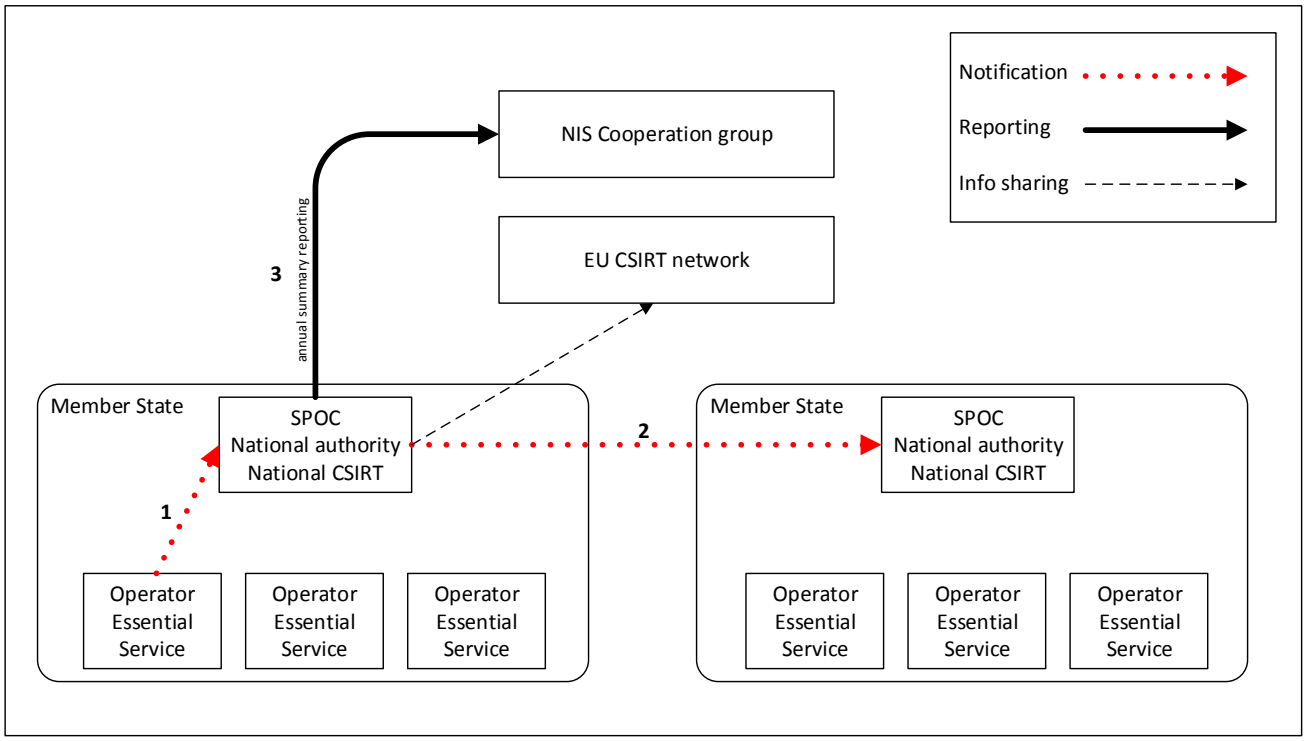

Figure 1 Mandatory incident notification requirements in Article 14

Note also that in the diagram, for the sake of simplicity, the three roles (the competent 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.

We give a few examples of incidents and notifications, illustrating the purpose of notification:

Example 1: Power cut causing payment gateway downtime: *Due to unknown issues there was a major power cut in one region of the country. The power cut would take a day to repair. The power cut caused a day of downtime of the IT systems of a payment gateway, affecting the entire country. A backup generator was without fuel and a failover mechanism failed to work correctly. The country uses electronic payments extensively so people across the country have problems taking public transport or buying food. The issue creates major disruptions and headlines across national media.*

Example 2: Container terminal disruption: *Unexpectedly the IT systems of a large container terminal in a port in the EU are suffering from a software bug. The issue happened overnight during regular system maintenance involving software updates. The computer systems suffer a full blackout and the container terminal comes to a standstill. The national authority receives the notification. The problems last almost a day causing severe disruptions to the country's transport sector and substantial losses to the economy. It takes weeks to recover the delays.*

A week after the incident is over the national authority asks the operator for a full report, explaining the root causes and the impact of the incident. The national authority decides to make also a public report, in collaboration with the operator. The public report explains the root causes, the total impact in terms of duration, the costs for society, and draws up lessons learned.

The underlying cause was a software update, which did not go as planned. Based on the report the national authority concludes that the operator did not have comprehensive change management procedures in place. The authority responsible for the sector decides to start a number of supervision activities around the topic of software change management, including a questionnaire survey and a workshop about the topic.

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 the incident. An outage seemingly caused by a software bug sometimes turns out to have been caused by a cyber-attack. A DDoS (distributed denial-of-service) attack may seem finished 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 OES 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[3].
- Assess the potential impact for essential services, citizens, the society, the economy, etc.
- Inform, in exceptional circumstances, and when this is 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 OESs, CSIRTs, etc.
- Inform authorities abroad when there is significant impact across the EU.

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

It is good practice to keep the first alert notification short and simple. 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 OES before taking actions.

4.2.2 Follow-up notifications

When the initial, alerting, notification happens, the affected operator often does not have the complete picture. The total duration and total impact of an incident is not known until the incident is resolved. Also the root cause of the incident may be unknown initially. 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 frequency of 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 affected 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 Operators of Essential Services

In this section we focus on the incident notification by the OES to the national competent authority and/or CSIRT, arrow 1 in Figure 1.

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 details 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.),
- plain paper.

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 multiple options, 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 some 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:

- **Encryption** – The information in the notification about the incident may be sensitive and 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.
- **Authentication**– Without authentication notification systems may receive fake notifications. It is important to do a sanity check, a double check, 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 encryption standards like StartTLS and DMARC, but not all organizations have adopted these. 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. Offering 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 S/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 a crisis situation, when internet connectivity or access to 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, online forms are 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 OES 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 OES 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 operator 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 OES 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 operator 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 OES 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 operator 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 operator 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 about cross-border impact

If a Member State receives a notification about an incident and there is significant cross-border impact, in one or more other EU Member States, then the single point of contact (SPOC) shall notify the SPOCs in the affected EU Member States.

Purpose: The purpose is to provide information relevant for the supervision activities of national authorities and/or CSIRTs when implementing Article 14.

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[4].

Procedure and format: This guideline does not propose a detailed procedure or template for the information sharing 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 State, 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 are advised to 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 MSs 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 an 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 State/s, should explain clearly how this information is to be handled by the receiving SPOC. Markings, labels, and handling instructions, like for instance the Traffic Light Protocol, could be used for this purpose[5].

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 contain 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 about the notified incidents to the NIS Cooperation Group. 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 14(3) and 14(5), 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:

- To create an EU-wide aggregation of notified cybersecurity incidents.

[4] 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.
[5] https://en.wikipedia.org/wiki/Traffic_Light_Protocol

- To identify trends, patterns in cyber security.
- To create 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 Voluntary notification

Member States should also allow organizations to notify cyber security incidents on a voluntary basis, even if they are out of scope of the NIS directive requirements. It is good practice to allow organizations to notify also incidents, which did not have a significant impact. Voluntary notifications should not impose any liability on the notifying party.

Voluntary reporting of incidents can help national authorities to get a better situational awareness and use the information provided to inform OES and other organisations of relevant new threats. It is good to keep in mind that an incident at an organization that is not an OES, can eventually have an impact on an OES, or otherwise on society or economy.

4.7 Informing the general public

After consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents. This could take place where public awareness is necessary in order to prevent an incident or to deal with an ongoing 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 includes a basic template for incident notifications. 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. As mentioned in section 4.4, this template could also be used by Member States as a template for information sharing in the case of cross-border impact.

- Nature of the incident
  - Type of threat or root cause that caused the incident, the general category (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
  - Sector or critical infrastructure affected
  - Essential service(s) affected
  - Description of the impact on the essential services
  - Scale of the impact on society and economy (see Annex A)
  - Geographic spread inside or outside the country
  - Number of citizens 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
  - 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 an example template for annual summary reporting, as non-binding guidance with regard to the information that the Single Point of Contact is required to submit to the NIS Cooperation

Group, every year, starting from 9 August 2018. This template (i.e. number of notifications, nature of notified incidents and actions taken in cross-border sharing of information) reflects the Directive's provision 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 OES 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 indicating the subsector
        - Electricity
        - Oil
        - Gas
        - Air transport
        - Rail transport
        - Water transport
        - Road transport
        - Banking
        - Financial market infrastructures
        - Health care
        - Drinking water supply and distribution
        - Digital Infrastructure
        - Other
    - 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 disruption of the essential service
    - If other Member States were impacted and informed

The information included in the report may be aggregated to avoid identification of OES in order to protect its interests.

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 or users 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 incident is significant until the moment it is no longer significant.

5.2.3 Rootcause category

Root cause categories are

- System failures (e.g. software bug, policy flaw, hardware failure, etc.)
- Natural disasters (e.g. storm, earthquake, etc.)
- Human errors (e.g. mistake, negligence, etc.)
- Malicious actions (e.g. cyber-attack, or other)
- 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