Department of
Finance
An Roinn
Airgeadais
www.finance-ni.gov.uk

GUIDANCE ON IMPLEMENTING THE NETWORK INFORMATION SYSTEMS REGULATIONS 2018

NETWORK INFORMATION SYSTEMS REGULATOR FOR NORTHERN IRELAND

JANUARY 2019

Purpose of the guidance

The purpose of this guidance is to provide an overview of the implementation of the Network and Information Systems Directive (the NIS Directive) in the energy, health, drinking water and transport sectors in Northern Ireland, following the coming into force of the Network Information Systems Regulations on 10th May 2018.

This guidance is aimed at those organisations that are designated as Operators of Essential Services (OES) under the NIS Regulations within the energy, health, drinking water and transport sectors in Northern Ireland.

This guidance details the responsibilities of OES as well as the roles and responsibilities of the regulator/competent authority (i.e. the body responsible for oversight and enforcement of the NIS Regulations within sectors) and how these will be carried out. It also sets out the process and thresholds for mandatory incident notifications.

This version of the guidance has been issued to assist Northern Ireland OES with compliance with the NIS Regulations. The guidance will be kept under review and will be updated to reflect views of the industry and to reflect learning gained from implementing the legislation. This will help ensure that the guidance is accurate, up-to-date and relevant. Additional guidance may be added to this document if necessary.

What is the NIS Directive?

The NIS Directive is designed to boost the overall level of security for network and information systems that support the delivery of essential services within the EU. It applies to those sectors which are vital for our economy and society, providing services such as the supply of electricity and water and the provision of healthcare and transport.

This NIS Directive was adopted by the European Parliament in July 2016 and came into force in August 2016, giving Member States 21 months to transpose it into their national laws.

The aim of the measures set out in the Directive is to improve the security of network and information systems across the EU by:

- Ensuring that Member States have in place a national framework to support and promote the security of network and information systems, consisting of a National Cyber Security Strategy, a Computer Security Incident Response Team (CSIRT), a national Single Point of Contact (SPOC) for other Member States and a NIS Competent Authority (or Authorities);

- Setting up a Cooperation Group and a CSIRT Network; the former to facilitate strategic cooperation and the exchange of information among Member States and the latter to promote swift and effective operational cooperation on incidents and sharing of information about risks;

- Ensuring that organisations within those vital sectors of our economy are effectively managing the security of their network and information systems. Organisations within those sectors that are identified by Member States as "Operators of Essential Services (OES)" will have to:

- take appropriate and proportionate technical and organisational measures to manage the security of their network and information systems (including managing cyber security risks and broader security and resilience risks to network and information systems);

- take appropriate measures to prevent and minimise the impact of incidents affecting the security of their network and information systems; and

- notify the relevant authority of any incidents affecting network and information systems which have a significant impact on the continuity of the essential service they provide.

In the UK, the NIS Directive applies to the following sectors: energy, health, water, transport and digital infrastructure. Some sectors are exempt where there are provisions within their existing legislation which are, or will be, at least equivalent to those the NIS Directive specifies (e.g. finance and civil nuclear sectors).

National Cyber Security Centre

The National Cyber Security Centre (NCSC) has several critical roles to play in support of NIS Directive implementation. It will be the CSIRT, the national SPOC and the national technical authority.

As the CSIRT, the NCSC will be responsible for incident response, including monitoring incidents, providing dynamic incident analysis and situational awareness as well as providing early warning alerts and announcements. These are not new functions for the NCSC as it already undertakes these roles at a national level for cyber security incidents.

As the SPOC, the NCSC will act as liaison on NIS Directive matters with the EU and between different national Competent Authorities. The role includes preparing a summary report of incident notifications and liaising with relevant authorities in other Member States on cross-border incidents.

As the national technical authority, the NCSC will be responsible for supporting OES and the Competent Authorities by setting security principles, publishing guidance, developing assessment tools and acting as a source of technical expertise on cyber security.

All of these roles are advisory; the NCSC will not have any regulatory responsibilities. It will not be able to, or seek to, enforce any actions on an OES. Enforcement will solely be the responsibility of the Competent Authorities.

As the national technical authority, the NCSC is responsible for two core products which support UK implementation of the NIS Directive. These are:

The NIS Security Principles and Guidance Collection

This comprises a set of outcome-based security principles which form part of the core requirements placed on OES to manage the security of their network and information systems.

The Cyber Assessment Framework (CAF)

This is a tool that provides a systematic method for assessing the extent to which OES are achieving the outcomes specified by the NIS principles. It can be used by Competent Authorities when assessing OES or by OES themselves as a self-assessment tool. The CAF provides Indicators of Good Practice against each element of the security principles in order to be able to assess the maturity of an OES against that particular element. The CAF has been revised following completion of pilot assessment exercises. A link is provided at Annex A.

Who is in scope?

The NIS Directive specifies the types of entities that all Member States should consider for inclusion (Annex 2 of the Directive). In the UK, designation of organisations as OES has be achieved through setting definitions and thresholds in legislation relating to the scale of an organisation's operations. The thresholds have been defined based on the level of societal or economic impact which could result from disruption to the services those entities provide. Organisations that meet those definitions and thresholds are automatically designated as OES. The definitions and thresholds for designating OES are contained in the NIS Regulations (see Annex A for a link to the full text) and have also been included in the section on certification thresholds below.

The NIS Regulations also provide Competent Authorities with the power to designate organisations in scope that do not meet these thresholds but are still considered to provide essential services. Competent Authorities are obliged to review the use of this designation power at regular intervals and the NIS Regulations also set out a process for OES to appeal such designations and request independent review.

Competent Authorities

Oversight and enforcement of the NIS Regulations is the responsibility of the designated Competent Authority.

The UK Government decided that a multiple competent authority approach was appropriate, with each Competent Authority having a detailed understanding of the individual sector/region and the associated challenges. Competent Authorities have, therefore, been designated for each sector or region covered by the NIS Regulations.

The Northern Ireland competent authority covers four sectors and several subsectors:

- Energy sector – all three subsectors electricity, gas and oil
- Health – the single healthcare settings subsector;
- Drinking water – the single drinking water subsector
- Transport – two of the four subsectors, rail and roads transport.

The only sectors where the NI competent authority does not have responsibility is the Digital Services Provision sector where Ofcom is the competent authority for the UK, and water and air transport where again there is a UK-wide competent authority.

The intention is to provide guidance for each sector in due course.

Competent Authorities have the sole authority and responsibility for all regulatory decisions in relation to the NIS Regulations. Competent Authorities will be supported by the NCSC as detailed in other parts of this document.

Responsibilities of the Competent Authority

Competent Authorities are responsible for:

- reviewing the application of the NIS Regulations in their sector or region;
- establishing the identification thresholds for the OES in their sector or region;
- preparing and publishing guidance to assist OES or Digital Service Providers in meeting the requirements of the NIS Regulations (including this guidance document);
- keeping a list of all OES who are designated and all revocations;
- assessing compliance of OES against the requirements of the NIS Regulations, including audits;
- determining the thresholds for notifiable incidents in their sectors or regions;
- receiving incident notifications;
- cooperating with other Competent Authorities to provide consistent advice and oversight to OES or Digital Service Providers;
- consulting and cooperating with the CSIRT, SPOC and Information Commissioner's Office (ICO);
- making sure that there are processes in place for responding to physical security incidents, system failures or natural hazards affecting network and information systems - and issuing guidance to support companies dealing with those types of incidents;
- investigating incidents;
- enforcement, including issuing notices and penalties, of the requirements of the NIS Regulations.

NI competent authority's interim approach to enforcement generally

The Regulator is aware that the NIS Regulations represent entirely new duties for many of the designated OES in scope. For some of them, this may be the first time they have been subject to any security regulation, or any regulation enforced by a competent authority. There is a requirement for NI (and UK/GB) departments to take a proportionate approach to any regulations they enforce and the Regulator will do so also in relation to the NIS Regulations. This is also reflected in regulation 23(1) of the NIS Regulations.

In relation to managing security risks, there should always be a continuous process of evaluating current risks and making appropriate changes to security measures as a result. Many designated OES will therefore be undertaking an ongoing process of security improvement; for some perhaps triggered or heightened by the introduction of the NIS Regulations. The Regulator understands that it will take time for OES to understand fully the practical application of their duties under the NIS Regulations, and that any required security improvements might take time to achieve and ongoing effort to maintain.

Compliance with the NIS will also mean the Regulator asking OES to carry out self-assessment against the Cybersecurity Assessment Framework before the end of the first year of operation of the NIS Regulations (by 9 May 2019). Given that the Regulations impose new duties on operators and a new way of reporting its activities, the Regulator wishes to discuss with operators how best this element of the Regulations might be achieved. The CAF is an extremely helpful document and has in-built guidance on how to comply with the NIS Regulations and ensure that existing systems are as robust as they should be. However, a full self-assessment against the CAF might an onerous exercise for some OES; the Regulator is ready to discuss options with OES that would ensure an assessment against the right criteria (as set out in the CAF) and in a way that will ensure maximum benefit for operators. On the other hand, OES may wish to carry out a full self-assessment against the CAF as this will provide a very good picture of where they stand in relation to compliance with the NIS Regulations.

Not all elements of the CAF will have the same relevance in all sectors so it is also important that OES do not pay undue attention to areas of low impact or little relevance to the robustness of networks and information systems; or do not pay enough attention to potential areas of vulnerability. It is important, therefore, that OES carry out scoping exercise to determine which networks and information systems are critical to the delivery of essential services. People at all levels of the organisation need to understand how their actions can lead to vulnerability in systems, but the initiative to secure network and information systems must come from the senior management and leaders in the organisation. IT staff will be critical to the success of the endeavours and they must be supported in their role, with clear lines of communication with line management and senior management to ensure that the right information is available to the right people.

Stepped approach to enforcement in relation to reportable incidents

The Northern Ireland Regulator will use a stepped approach to enforcement when an OES is found to be failing to meet requirements. This relies heavily on a collaborative approach between the regulator and OES. Any enforcement, particularly the issuing of penalties, will be a last resort and in all cases will be proportionate to the failing identified.

The stepped approach that will be taken in the Northern Ireland sectors may be summarised as follows:

Step 1: Advise and persuade

When any deficiencies are identified, the initial approach taken by the Regulator will be to engage and discuss this with the OES. This will include discussing what the failing or deficiency is and how and when it can be addressed. The Regulator will agree the remedial actions proposed by the OES and when these actions should be completed. The Regulator may wish to follow-up with further assessments or audits to ensure that these actions have been taken and any failings have been addressed appropriately and proportionately.

A stronger line may be taken if these actions fail to be addressed in the agreed timeframe although this can still stop short of any formal enforcement action.

The Regulator may issue information notices requiring the OES to provide specified information to support compliance assessment.

Step 2: Enforcement notice
Where the initial collaborative approach has not worked and it is clear that failings are not being addressed, a formal enforcement notice will be issued. This will set out the failings identified, the steps to be taken and the time period in which they need to be completed.

Step 3: Penalty notice
Where the OES has failed to take adequate steps to rectify a failure identified in an enforcement notice a monetary penalty may be issued. In practice such a step is likely to be taken only in extreme cases and as a last resort where the initial actions taken by the Regulator have not been successful at instigating appropriate action by the OES.

In determining the value of the monetary penalty, the Regulator will consider the appropriate and proportionate level within the prescribed limit of £17m.

Compliance regimes operated by other regulators or oversight bodies will continue in parallel with this approach. The Regulator will engage directly with other regulators and oversight bodies to ensure that the regulatory regime is as efficient as possible.

It is possible that enforcement action could be taken under both the General Data Protection Regulation (GDPR) and NIS because these are separate legislative regimes with differing legal requirements. This will apply not just to GDPR but other sectoral and general legislation. However, the NIS Regulations make provision, at regulation 23, for Competent Authorities to consider whether enforcement action is reasonable and proportionate on the facts and circumstances of the case, including consideration of whether a contravention is also liable to enforcement under another enactment. The regulator will liaise closely with the Information Commissioner on implementation of the NIS Regulations particularly if a reportable occurs that could be reportable or actionable under both sets of legislation.

It should also be noted that regulation 19 of the NIS Regulations sets out a process for OES to request independent review of penalty decisions taken by the Competent Authority. Further guidance will be developed on this aspect of the Regulations.

Incident investigation – approach that will be taken following an incident

As has been set out in section 4 of this document, all OES must notify the Regulator of incidents that meet the designated thresholds. Following the notification, and allowing for a period of resolution and recovery, the Regulator will decide whether or not the incident requires further follow-up investigation. This may include requesting further details of the incident.

The purpose of these investigations could be to: i) establish the cause of the incident and assess whether the incident was preventable; ii) assess whether effective and reasonable risk management was in place; iii) assess whether the operator had appropriate security measures in place; and iv) assess how the OES responded to and managed the incident.

Once the investigation has concluded, the Regulator will decide on any appropriate next steps, which could be no action, advice or formal enforcement action.

It is expected that OES will also conduct their own investigations and this will form the basis for the conversation between the Regulator and the OES. The Regulator may require additional information and in some cases may instruct the OES to appoint a third party investigator and/or auditor from an approved list. Where this type of action is required, the intention is that it will be the responsibility of the OES to contract the third party and pay the costs. The results of such investigations/audits should be shared with the Regulation to determine if further action is required. Further advice will be prepared on this aspect of implementation of the Regulations.

It should be noted that simply having an incident is not usually itself an infringement of the NIS Regulations and therefore, does not automatically mean enforcement action will be taken. A key factor for determining whether enforcement action is required will be whether proportionate security measures and procedures were in place and being followed and whether the OES has responded to any earlier recommendations made by the Regulator, for example, where the Regulator has conducted a post-incident investigation. Not having notified the Competent Authority of an incident that meets the incident notification thresholds would be an infringement of the NIS Regulations.

Network Information Systems Regulator for Northern Ireland

The Department of Finance has been designated the competent authority in Northern Ireland. The authority has a wide remit with responsibilities in four sectors as set out in the table below:

The NI competent authority is both a sectoral and regional one with a wider span of responsibility than any other UK competent authority. The sectors covered by the NI Regulator come within the functions of three Northern Ireland Departments as follows:

- Department for the Economy: energy sector – electricity, oil and gas subsectors
- Department of Health: health sector;
- Department for Infrastructure: transport sector – rail and roads subsectors; and the drinking water distribution and supply sector.

The NI Regulations include an information sharing provision that allows the regulator and the relevant departments to share information relevant to operation of the Regulations.

The NI competent authority will seek to draw on best practice from other competent authorities while operating as a single regulatory body across a number of industries in the region. Over time it is anticipated that sector-specific guidance will be issued and this will assist operators in understanding the requirements of the Network Information Systems Regulations 2018 and the significance of the cyber assessment framework for their organisation and subsector.

Designation of Northern Ireland operators of essential services

Under the Network Information Regulations 2018 operators of essential services are deemed to be covered by the legislation if they meet certain criteria or certification thresholds. Schedule 2 of the Regulations set out these certification thresholds and these are summarised in the table below for ease of reference:

TABLE 1 - SECTORS AND SUBSECTORS COVERED BY NI COMPETENT AUTHORITY AND NUMBER OF OPERATORS DEEMED TO BE INCLUDED

SECTOR*	SUBSECTOR & LEGISLATION RELEVANT TO THRESHOLDS	CERTIFICATION THRESHOLDS FOR OPERATORS IN NI	NI OES
	Electricity Electricity (NI) Order 1992	*Generation* Licence holder under Art 10(1)(a) 1992 Order plus generate ≥350 mw	2
		Transmission Licence holder under Art 10(1)(b) 1992 Order	3
		Distribution Licence holder under Art 10(1)(bb) 1992 Order	1
		Supply Licence holder under Art 10(1)(c) 1992 Order plus >8000 customers	7
		Single Energy Market operator Licence holder under Art 10(1)(d) 1992 Order	1
	Gas Gas (NI) Order 1996	*Transmission* Licence holder under Art 8(1)(a) 1996 Order	8
		Storage Licence holder under Art 8(1)(b) 1996 Order	1
		Supply Licence holder under Art 8(1)(c) 1996 Order plus >2,000 customers	4
		Liquefied natural gas (LNG) Licence holder under Art 8(1)(d) 1996 Order	0
	Oil	*Storage* Capacity to store >50,000 tonnes crude oil	7
Transport**	**Rail**	*Operation of a rail network* Any rail network	1

	Roads	*Operation of a road network* 50 billion vehicle miles travelled per year	0
Health	**Healthcare settings**	*Operation of a health and social care trust* Any Health and Social Care Trust	6
Drinking water supply & distribution	**Drinking water supply & distribution**	*Supply and distribution of potable water* Supply to 200,000 people or more	1

*The NI Competent Authority does not cover the Digital Infrastructure sector - CA for the UK is Ofcom

**The NI CA does not cover the air transport and water transport subsectors: CAs for the UK are SoS for Transport and CAA (air) and SoS for Transport (water)

NI competent authority's maintenance of lists of designations, including their review

As already noted above, NI competent authority must keep a list of all the OES who are designated, or deemed to be designated, under regulation 8, including an indication of the importance of each operator in relation to the subsector in relation to which it provides an essential service.

NI competent authority is required by regulation 8(9) to review that list at regular intervals, the first of which must take place before 9th May 2020, and subsequent reviews taking place biennially.

NI competent authority's powers to revoke OES designations

NI competent authority has the power under regulation 9(1) to revoke a deemed OES designation falling within the three above-mentioned three categories, if it concludes that an incident affecting the provision of that essential service is not likely to have significant disruptive effects on the provision of the essential service.

Before revoking any designations, the Regulator must under regulation 9(3):

- serve a notice in writing of proposed revocation on the designated entity;
- provide reasons for the proposed decision;
- invite the entity to submit any written representations about the proposed decision within such time period as the regulator may specify; and
- consider any representations submitted by the entity before a final decision is taken to revoke the designation. 4.32 The way in which NI competent authority revoke designations is by notice in writing served on the person who has been designated in accordance with regulation 24 of the NIS Regulations.

OES security duties

Regulation 10 of the NIS Regulations imposes on designated OES the following security duties: i) "(1) An OES must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies.

ii) (2) An OES must take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services.

iii) (3) The measures taken under paragraph (1) must, having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risk posed.

iv) (4) Operators of essential services must have regard to any relevant guidance issued by the relevant competent authority when carrying out their duties imposed by paragraphs (1) and (2)."

In that regard, the regulator notes that, as required by regulation 10(3), the measures to be taken under regulation 10(1) by designated OES for the digital infrastructure subsector must ensure a level of security appropriate to the risk presented "having regard to the state of the art" and, therefore, any compliance assessment by the regulator would have regard to the state of the art of such measures.

OES duties concerning security incident reporting
Notifiable NIS incidents

Regulation 11(1) of the NIS Regulations imposes on designated OES in the digital infrastructure subsector a duty to report to NI competent authority any incident which has a significant impact on the continuity of the essential service which it provides (i.e. **"a NIS incident"**). Such reporting should be done "*without undue delay and in any event no later than 72 hours after the operator is aware that a NIS incident has occurred*" and "*in such form and manner as* [NI competent authority] *determines*" (regulation 11(3)(b)).

In determining the significance of the impact of an incident, an OES must under regulation 11(2) have regard to the following factors:
- the number of users affected by the disruption of the essential service;
- the duration of the incident;
- the geographical area affected by the NIS incident; and
- any relevant guidance issued by NI competent authority.

The regulator is required under regulation 11(5) to assess whether any further action is required in respect of a reported NIS incident and to share the NIS incident information with the NCSC, in their role as the UK CSIRT, as soon as reasonably practicable.

The regulator is further required under regulation 11(9) to provide a report to the SPOC identifying the number and nature of NIS incidents notified to us. Our first report must be submitted on or before 1st July 2018 and subsequent reports must be submitted annually.

NI competent authority's process requirements for security incident reporting

Regulation 11(3)(a) lists the essential requirements to be included by OES in a report to NI competent authority, namely the report must provide the following information:

- the operator's name and the essential services it provides;
- the time the NIS incident occurred;
- the duration of the NIS incident;
- information concerning the nature and impact of the NIS incident;
- information concerning any, or any likely, cross-border impact of the NIS incident; and

any other information that may be helpful to NI competent authority. 4.41 However, that information is limited to information which may reasonably be expected to be within the knowledge of that OES (regulation 11(4)).

As noted above, security incident reporting must be done in such form and manner as NI competent authority determines and OES must also have regard to any relevant guidance issued by NI competent authority when OES carry out their duties imposed by regulation 11(1) to (4).

****IMPORTANT NOTE:** In that regard, it should be noted that NIS incident reports should be submitted to NIS.CA@finance-ni.gov.uk

Such reports should be submitted on the form attached at Annex B, including as much information as is reasonably available at the time of reporting. Noting that the duty imposed on OES to report "without undue delay", and in any event within 72 hours of the OES becoming aware of the NIS incident, it is possible that complete information will not be available at the time of the report. In such cases, additional information should be provided as it becomes available, but meanwhile the OES in question should not withhold reporting until more complete information is available.

****IMPORTANT NOTE:** OES should also provide NI competent authority with a general NIS incident contact point for enquiries about incidents which the regulator becomes aware of, but which have not yet been reported.

OES should note that, like the other designated regulators for the NIS Regulations, NI competent authority's role does not include incident response. OES should therefore not view NIS incident reporting to us as any substitute for reporting to other agencies which provide specific support. As such, OES, and indeed any other companies in the sector suffering from a cyber security incident with which they require assistance or technical support, should contact the NCSC through the usual channels, as soon as possible. Similarly, if the incident may be criminal in nature, the appropriate law enforcement agency should be contacted.

NI competent authority's guidance on the significance of the impact of an incident (i.e. reporting thresholds)

****IMPORTANT NOTE:** As noted above, one of the factors that OES must have regard to in determining the significance of the impact of an incident is any relevant guidance issued by NI competent authority. The regulator has set out in the table below our initial view of the thresholds at which NIS incidents will have a significant impact and they should therefore be reported to NI competent authority.

The Regulator will review this first set of thresholds with DCMS, the NCSC and individual OES as they identify themselves to us. The regulator expects that there will be a need to refine them based on these discussions in any revised guidance.

The Regulator understands that putting in place processes to ensure qualifying incidents are reliably reported is likely to take some time for the OES. Meanwhile, the regulator would encourage all the designated OES to make their best efforts to report relevant incidents. The Regulator would expect that they will not adopt an unduly restrictive approach to interpreting these criteria – our general guidance is that, if there is any doubt as to whether (or not) a criterion is met, the OES should submit a report to NI competent authority

ANNEX A

Tables of specific reporting thresholds

Health sector - Incident Notification Thresholds

	NEGLIGIBLE
	SYSTEMS: Critical systems and services not involved. Key administrative IT systems not involved. **PEOPLE**: Patients: patient care not impacted. Staff: HSC Trust staff not impacted. Population: 0%-10% local population impacted. **DURATION**: Peripheral systems and services interruption of less than 1 day. **GEOGRAPHY:** Impact limited to part of an HSC Trust. **REPUTATION**: No impact on the reputation of HSC. Possible local media interest
	MINOR
	SYSTEMS: Critical Systems & Services not involved; patient care not impacted. Key administrative IT systems not involved. **PEOPLE**: Patients: patient care not impacted. Staff: HSC Trust staff not impacted. Population: 0%-10% local population impacted. **DURATION**: Peripheral systems and services interruption of more than 1 day but less than 5 days. **GEOGRAPHY**: Impact limited to part of an HSC Trust. **REPUTATION**: No impact on the reputation of HSC. Possible local media interest
	SIGNIFICANT
NIS REPORTABLE	**SYSTEMS**: Temporary loss of critical systems and services. Has the potential to disrupt the continued operation of the health board or delivery of health services. Key administrative IT systems not involved. **PEOPLE**: Patients: patient care impacted. Staff: HSC Trust staff not impacted. Population: 0%-10% local population impacted. **DURATION**: Critical systems and services interruption and patient care disrupted for less than 1 day. **GEOGRAPHY**: Significant impacts widely across an HSC Trust. **REPUTATION**: Could have a negative impact on the reputation of HSC. Possible local media interest
	MAJOR

NIS REPORTABLE	**SYSTEMS**: Critical systems and services failure. Key administrative IT systems performance impaired. **PEOPLE**: Patients: patient care significantly impacted. Staff: HSC Trust staff inconvenienced. Population: 10%-50% local population impacted. **DURATION**: Critical systems and services failure interrupts continued operation of the HSC Trust or delivery of health services for more than 1 day but less than 5 days. **GEOGRAPHY**: Significant impacts across the entire HSC Trust. Wider geographic spread; likely that other HSC Trusts may experience a similar attack, or that the incident could spread to those organisations. **REPUTATION**: Local & national media interest. Negative impact on the reputation of local HSC Trust; reputational damage to HSC

	EXTREME
NIS REPORTABLE	**SYSTEMS**: Significant loss of critical systems and services. Major disruption to administrative IT systems. **PEOPLE**: Patients: patient care significantly impacted. Staff: Significant impact and inconvenience to HSC Trust staff. Population: Over 50% local population impacted. **DURATION:** Critical systems and services failure disrupts the continued operation of the HSC Trust or delivery of health services for more than 5 days. **GEOGRAPHY**: Significant impacts across the entire HSC Trust. Majority of HSC Trusts similarly impacted. **REPUTATION**: National media interest. Negative impact on the reputation of impacted HSC Trusts and on the HSC as a whole.

Tables of specific reporting thresholds

TRANPORT SECTOR Incident Notification Thresholds

Rail transport subsector

- A single incident which results in 30% of a train operator's services being cancelled in a 24-hour period or in an amended timetable being run that is equivalent to that number of cancellations;

- A single incident which results in more than 20,000 delay minutes over a period of one week or in an amended timetable being run that is equivalent to that number of delay minutes.

Road transport subsector

- No thresholds have been set because no operators are deemed to be included according to the certification threshold set out in the NI Regulations 2018 of 50 billion vehicle miles travelled per year.

Tables of specific reporting thresholds

Drinking water distribution and supply Incident Notification Thresholds

Drinking water quality: a. Do not drink b. Boiling advice	Health risk: >500 properties >10,000 properties
Discoloured water/taste and odour	>10,000 properties
Loss of supply: a. Less than 3 hours b. Greater than 3 hours c. Greater than 6 hours d. Greater than 12 hours e. Greater than 24 hours	 N/A N/A >40,000 properties >40,000 properties >40,000 properties

Tables of specific reporting thresholds

Energy Sector Incident Notification Thresholds

Sector/subsector	**NI Incident Threshold**
Electricity Generation	The unauthorised or unplanned loss of ≥350MW of electricity generation, when cumulated with all generators operated by affiliated undertakings
Electricity Transmission	Loss of supply or outage that has or is likely to lead to loss of supply to grid supply points and affects customers for more than 3 minutes
Electricity Distribution	Unplanned single incident loss of supply to 8,000 customers for more than 3 minutes
Electricity Suppliers	Unplanned shut off or single incident loss of supply to 8,000 customers for more than 3 minutes
Electricity Interconnectors	The net unauthorised or unplanned loss or gain of ≥560MW of interconnector flow in a given direction
Gas Transmission	Loss of supply or outage that has or is likely to lead to loss of supply to offtakes and affects customers
Gas Distribution	Unplanned single incident loss of supply to 2,000 customers
Operation of gas storage facilities	Unplanned loss of conveyance >8,219 tonnes oil equivalent over 24-hour period
Oil storage	Loss of supply that affects >2,000 customers

Annex B

Points to capture

Name of person reporting
Role in the company
Phone
Email
Name of the Organisation and the essential service it provides
Internal incident ID number or name
Date and time incident detected
Date and time incident reported
Type of incident
Cyber / non-cyber / both
Incident status
Detected incident / suspected incident
Incident stage
Ongoing / ended / ongoing but managed
Please provide a summary of your understanding of the incident, including any impact to services and/or users, including:

- Incident type
- Description of the incident
- How the incident was discovered
- Duration
- Location of the incident(s)
- Services/systems affected
- Impact on those services/systems
- Impact on safety to staff or public
- Suspected cause
- Whether there is any known or likely cross-border impact
- Any other relevant information