Ofcom's changes to the guidance on incident reporting thresholds for the digital infrastructure subsector

Decision to revise Ofcom's Guidance under the Network and Information Systems (NIS) Regulations 2018

STATEMENT:

Publication date: 31 May 2023

Contents

Section

1. Overview

Ofcom is the designated competent authority for the digital infrastructure subsector in the United Kingdom under the Network and Information Systems Regulations 2018 (more commonly referred to simply as the **"NIS Regulations"**). As part of our role, we prepare and publish statutory guidance in relation to that subsector under the NIS Regulations, and operators of essential services (**"OES"**) for that subsector must have regard to this guidance in complying with their statutory duties.

We published a consultation on 1 November 2022 in which we proposed to update our NIS Guidance, focusing on the incident reporting thresholds. We received three responses, which are published on our website. After considering the responses, we are now publishing our final statement, together with our revised NIS Guidance.

What we have decided – in brief

We have changed our NIS Guidance with lowered incident reporting thresholds.

This means that we expect the OES in the digital infrastructure subsector to report incidents to us which have a lower level of impact on their services than was previously the case. This should result in more incidents being reported to us than would have occurred under our previous guidance.

In deciding to make this change, we have taken into account factors such as the increased importance of the services we oversee since we set the previous thresholds, the Government's National Cyber Security Strategy: 2022 to 2030, and the responses we received to our consultation.

We have also made the proposed change to include a reference to our Regulatory Enforcement Guidelines.

The previous version of our NIS Guidance included a section setting out how we would approach enforcement action in cases relating to failure to comply with the requirements of the NIS Regulations. In December 2022, we published Ofcom's Regulatory Enforcement Guidelines which cover the relevant aspects of the NIS Regulations.

We have published our revised guidance alongside this statement.

2. Our consultation proposals

2.1 In this section, we summarise our two main proposals to change our NIS Guidance for the OES in the digital infrastructure subsector.

Proposed new incident reporting thresholds

2.2 Regulation 11(1) of the NIS Regulations imposes a statutory duty on OES to notify us in writing of "any incident which has a significant impact on the continuity of the essential service which that OES provides" ("a NIS incident").

2.3 We explained in the consultation the three factors set out in regulation 11(2) to which OES must have regard in determining the "significance" of the impact of an incident, namely, the number of users affected by the disruption of the essential service, the duration of the incident and the geographical area affected by the incident.

2.4 We noted[1] in our consultation that, while OES must have regard to our NIS Guidance on incident reporting thresholds, the statutory duty on OES is to report any incident having a "significant impact" by reference to those three factors. Therefore, we clarified that an incident must be reported to us if it has a significant impact by reference to those factors irrespective of what our incident reporting thresholds state in our NIS Guidance from time to time. However, we also noted[2] that our proposed new incident reporting thresholds sought to give OES clarity and certainty about our own expectations of what generally is likely to constitute a significant incident with regards to those factors.

2.5 Considering the nature of the digital infrastructure subsector, the OES often does not have a direct relationship with the end users of the service. For example, end users may be using an internet access service, and the provider of that service in turn is, to some extent, relying on the services provided by the OES to deliver it. Thus, it may not be feasible for an OES to determine the exact number of users impacted.

2.6 For that reason, our existing incident reporting thresholds use various volume metrics as proxies to estimate the number of users potentially affected by the disruption of the essential service. In particular, for the different types of OES within the digital infrastructure subsector:

- for TLD Name Registry Services and DNS Resolver Services, the threshold refers to the impact on the number of queries that the OES can process in a given period of time.
- for DNS Authoritative Hosting Services, the threshold refers to the impact on the number of registered domains for which the service can be provided; and
- for IXP Services, the thresholds refer to the impact on connectivity for Autonomous System Numbers (ASNs) or port.

[1] Paragraph 2.6 of our consultation.
[2] Paragraph 3.37 of our consultation.

2.7 The geographical area affected by a disruption to the continuity of essential service within the UK, will typically be considered as nationwide for the case of TLD, DNS Resolvers and DNS Authoritative Hosts. In the case of IXPs, typically their services and networks are regional, and therefore the impact of an incident would normally be expected to be across the region within which they operate and potentially nationwide. For example, for a London-based IXP, the impact is likely to be for London and potentially nationwide, for a Manchester-based IXP, its impact is likely to be for Manchester, as a starting point.

2.8 In the consultation, we proposed lowering both the volume and duration of the impact of an incident before we consider it is likely to have had a significant impact on the service, and therefore be reportable. Table 1 below sets out our new incident reporting thresholds, as proposed in our consultation.

Table 1: Summary of existing incident reporting thresholds and Ofcom's new incident reporting thresholds as proposed in our consultation

Existing thresholds			Proposed thresholds		
Essential service for this subsector	Metric	Service degradation (Time)	Metric	Service degradation (Time)	Service degradation (Volume)
TLD Name Registry Service	Loss or significant degradation of >= 50% of aggregated name resolution capability (measured in queries per second)	1 hour	Loss or significant degradation of >= 25% of aggregated name resolution capacity (measured in queries per day)	>=15 mins	>= 25%
DNS Resolver Service	Loss or significant degradation of service to >= 50% of aggregated DNS Resolver capacity (measured in queries per second)	30 minutes	Loss or significant degradation of service >= 25% of aggregated DNS Resolver capacity (measured in number of different IP addresses handled per day)	>=15mins	>= 25%
DNS Authoritative Hosting Service	Loss or significant degradation (e.g. serving incorrect results) of service for >=50% of registered domains	1 hour	Loss or significant degradation (e.g. serving incorrect results) of service >=25% of aggregated Authoritative	>=15 mins	>= 25%

			Hosting capacity (measured in queries per day)		
IXP Service	**Loss or significant degradation of connectivity to 25% of connected Autonomous System Number (ASN); OR** **Loss of >= 90% of total port capacity**	**1 hour**	**Loss or significant degradation of connectivity to >= 25% of connected Autonomous System Number (ASN); or** **Loss of >= 50% of total bandwidth capacity across all ports.**	**>=15 mins**	**>= 25% for ASN** **or** **>= 50% for total bandwidth capacity across all ports**

Proposed updated referencing to our Enforcement Guidelines

2.9 In our consultation, we also proposed to make another, minor, change to the NIS Guidance. Our previous version of the NIS Guidance included a section setting out how we would approach enforcement action in cases relating to failure to comply with the requirements of the NIS Regulations. This referred to relevant parts of another document, Ofcom's Enforcement Guidelines, which was current at the time. This document set out Ofcom's approach to enforcement in detail but predated the NIS Regulations and hence did not make reference to them.

2.10 In December 2022, we published Ofcom's Regulatory Enforcement Guidelines which replaced our previous Enforcement Guidelines. This new document now includes the relevant aspects of the NIS Regulations within its scope. That document therefore replaces our previous guidance on this matter in the NIS Guidance. We therefore proposed updating this section accordingly, by removing the superseded content and replacing it with a reference to the 2022 Regulatory Enforcement Guidelines.

3. Summary of responses and our decision

3.1 We received a total of three responses to the consultation, all of which are non-confidential and are published on our website. We have set out a summary of the respondents' comments below, followed by Ofcom's response. In general, all respondents supported the view that the incident reporting thresholds needed to be reviewed.

Responses to the consultation

Geographic impact on vulnerable communities

3.2 Citizens Advice Scotland (CAS) stated that due to Scotland's geography, when a communications outage occurs, the impact on rural and island communities is proportionately much greater than other areas.

3.3 CAS stated that under each of the three measures for assessing significance – number of users, duration, and geographical area – an entire island community, or group of islands, could potentially lose connectivity without this being deemed a significant incident. CAS also stated that, when finalising the threshold values, careful consideration should be given to how the incident reporting thresholds could be amended to reflect the severe impact of outages in vulnerable rural and island communities. For example, rather than grouping island communities by geographical area or population levels, Ofcom could consider requiring IXP services to consider each island or vulnerable rural community individually; perhaps by creating a special category of 'vulnerable community' within the reporting framework.

Estimating potential impact

3.4 LINX supported the proposed new thresholds but went on to describe the difficulty of predicting which customers will be affected by disruptions to the services in scope of the digital infrastructure subsector of the NIS Regulations. This is because they tend not to be restricted to regional, or often even national geographic, boundaries.

3.5 LINX said that using the metric "potential impact in a worst-case scenario" is not useful as it does not give an indication of the number of users actually affected by an incident. They are unable to determine the actual number of users and actual regions impacted by an incident in the case of an IXP site outage.

3.6 LINX recognised that determining the potential UK impact in the event of the failure of one of their London operational facilities is difficult, thus it would welcome Ofcom conducting detailed research regarding the aggregate Internet communications infrastructure in the UK. They also said that they agree that a precautionary approach justifies regulatory oversight, and a careful watch should be maintained on material incidents as they occur, and close attention paid to any observable effects.

Incident duration thresholds

3.7 While supporting the modified thresholds, Nominet expressed a concern that the use of queries per day does not seem appropriate when looking at service performance over a 15-minute time period. In addition, Nominet stated they did not understand the proposal to move away from queries per second.

Redundant capacity

3.8 Nominet stated that when it comes to measuring available capacity, their DNS services operate with very high levels of inherent redundancy (>99%) so a reduction in capacity of 25% as proposed may well not actually result in a significant service degradation.

Ofcom responses and decision on new incident reporting threshold

3.9 Our existing thresholds for incident reporting in our NIS Guidance for the digital infrastructure subsector have been in force from 2018. Since then, there has been no update to these thresholds for over four years.[3] In light of the increased dependence on essential services in the digital infrastructure sub-sector for the functioning of the internet, benefit to the wider economy, including societal wellbeing, the digital infrastructure subsector has become increasingly critical and we now consider that it is the right time for revising those thresholds considering such dependencies, which we discuss below.

Growth and increased reliance on essential services in the digital infrastructure sector

3.10 The internet relies on the optimal operation and availability of services in the digital infrastructure subsector (e.g. DNS Top Level Domain (TLD) Name Registry services, DNS Resolver services, DNS Authoritative Hosts services and Internet Exchange Point ("IXP") services).

3.11 The high dependency on these services for the running of the internet has been further highlighted in recent times. For example, the Covid Pandemic has shown that internet-based services were vital in accessing a variety of important services for the public, such as NHS and GP services, financial services, remote/home working, online shopping, schooling and other educational content. These services now play a vital role in the functioning of the UK economy and they are important for overall societal wellbeing.

3.12 Critical services across the UK are increasingly dependent on digital infrastructure services as they adopt digital technologies or move to the cloud. For example, an incident in the digital infrastructure subsector can result, for example, in significant outages of communications applications, ticketing systems in the transportation sector, or failure of safety systems which are cloud based.

[3] They were included in our Interim NIS Guidance from 8 May 2018. Our existing NIS Guidance was updated on 5 February 2021, but our incident reporting thresholds were not substantively changed.

3.13 Furthermore, communications providers[4] (CPs) all have an increased dependency on digital infrastructure services, something which we expect will significantly increase as more telecom infrastructure is migrated to cloud technologies, particularly if any part of their services are delivered through or dependent on public cloud services via the internet. We also expect CPs to increase their adoption of Software as a Service (SaaS) based applications or services (Business Support Systems (BSS) e.g. Customer Relation Management (CRM), Enterprise Resource Planning (ERP)) and Operational Support Systems (OSS) e.g. Customer provisioning, billing, Privilege Access Management (PAM), or Configuration Management Database (CMDB), as part of the digital transformation trend, migrating away from on-premise data centres to the public cloud based subscription services to improve time to market and reduce cost[5].

3.14 Number-Independent Interpersonal Communications Services (or "NIICS") and collaboration platforms like Microsoft Teams, WhatsApp and Zoom all rely on DNS and IXP digital infrastructure to deliver Voice Over IP (VoIP), Instant Messaging and video calls. Such services have become essential to economic and social activity since the pandemic in allowing activities such as home working, education and delivery of health care.

Ofcom expectations on incident reporting thresholds

3.15 Against that background, we consider that it is necessary to, in effect, lower the existing incident reporting thresholds, to give OES clarity and certainty about our expectations of what constitutes as a significant incident with regards to the factors referenced in regulation 11(2) when considering reporting incidents to us pursuant to their statutory duties under regulation 11(1).

3.16 The incident reports are an important source of information for Ofcom to assess the impact on UK users, OES compliance to fulfilling their duties, the need for subsequent investigations or inspections and for provision of improved and relevant guidance to OES. Such reports would also enable us to identify any specific gaps in the technical and organisational measures that OES must take under regulation 10 of the NIS Regulations to manage risks posed to the security of the network and information systems on which their essential service rely.

3.17 Ofcom understands the importance of the points raised by CAS regarding the potential impact of communications outage or disruptions on rural and island communities. We note, however, that due to the nature of the services offered by OES in the digital infrastructure subsector, incidents do not tend to have geographically focussed impacts, and, where they do, these impacts are difficult for the OES themselves to predict. Indeed, a similar point to that effect was made by LINX in their response (see above).

3.18 We consider that CAS's points are more directly relevant to incidents affecting telecoms connectivity, and hence to the services offered by Communications Providers (CPs), rather

[4] By CPs, we specifically refer to persons who provide an electronic communications network or an electronic communications service.
[5] https://inform.tmforum.org/future-oss-bss/2020/08/saas-the-new-revolution-in-telecom-bss/

than OES. These sorts of services are covered by our work under section 105A-Z of the Communications Act 2003. These services are not in the scope of the NIS Regulations, nor the incident reporting thresholds to which this consultation relates.[6]

3.19 We acknowledge LINX's points relating to the difficulty in estimating the actual impact of an incident on the end users, and geographical coverage, of an essential service. We note, however, that OES are required by the NIS Regulations to report incidents which have a significant impact on the continuity of their essential service, having regard to factors including the number of users, duration of incident and the geographical area affected. The thresholds in our NIS Guidance are intended to explain Ofcom's general view on incidents which are likely to meet these criteria. It is because of the difficulty of estimating these factors directly, that our thresholds, both in our previous and our revised NIS Guidance, use proxies for these factors, and are generally based on a potential worse case impact.

3.20 We also note here that our NIS Guidance encourages OES to submit an incident report in the event there is any doubt as to whether a threshold has been met.

3.21 Based on the feedback received from Nominet, we have decided to retain the existing use of queries per second in the relevant thresholds.

3.22 The proposal to move away from queries per second to queries per day was intended to better cover the scenario where repeated incidents with the same underlying cause occur over a period of time, which, in aggregate, would have exceeded the incident reporting thresholds. We consider that such incidents are likely to be, in effect, a single incident but with their impact occurring over an extended period of time. Repeat incidents of this nature can have a significant impact on end users, so it is important we consider why they happen, how they are managed, and the steps taken to reduce further reoccurrence. As such, we expect such incidents should be reported as a NIS incident. We have added the following clarification on this point to the NIS Guidance:

- *"For repeat incidents, where multiple incidents occur within a four-week period resulting from a single underlying cause, the aggregate impact should be considered for reporting purposes."*

3.23 This approach is in-line with our approach for the reporting of similar repeat security incidents under section 105K of the Communication Act 2003[7].

3.24 In relation to Nominet's point about its redundant capacity, in setting our thresholds we have considered the impact to the essential service's capacity available to customers, rather than any redundant systems. Ofcom will expect to receive a report if an incident affects the current operating capacity, or the service's capacity available to customers, in accordance with the incident reporting thresholds. For the avoidance of doubt, a planned

[6] For ease of reference, our guidance on incident reporting for CPs, under their Communications Act 2003 obligations (Annex 1 - General statement of policy under section 105Y of the Communications Act 2003 (ofcom.org.uk)), and on the resilience of these networks and services (Annex 2 - Ofcom guidance on resilience requirements imposed by or under sections 105A to D of the Communications Act 2003) are available on our website.

[7] See footnote on page 24 of our "General statement of policy under section 105Y of the Communications Act 2003"

outage, such as maintenance within a predefined time window, is not a reportable incident.

3.25 In light of the above considerations, we have decided to adopt our new incident reporting thresholds as set out in the consultation, with the modifications explained above. We are publishing our revised guidance alongside this statement, which includes the new thresholds, shown below, at new Table 1 of that guidance.

Table 2: Summary of Ofcom's New Incident Reporting Thresholds

Essential service for this subsector	Metric	Service degradation (Time)	Service degradation (Volume)
TLD Name Registry Service	Loss or significant degradation of aggregated name resolution capacity (measured in queries per second)	>=15 mins	>= 25%
DNS Resolver Service	Loss or significant degradation of aggregated DNS Resolver capacity (measured in number of different IP addresses handled per second)	>=15mins	>= 25%
DNS Authoritative Hosting Service	Loss or significant degradation (e.g. serving incorrect results) of aggregated Authoritative Hosting capacity (measured in queries per second)	>=15 mins	>= 25%
IXP Service	Loss or significant degradation of connectivity to connected Autonomous System Numbers (ASN); or	>=15 mins	>= 25% or
	Loss of total bandwidth capacity across all ports.		>= 50%

3.26 In reaching this decision, we have taken into account the matters we discussed in our consultation, including factors such as the increased importance of the services we oversee since we set the previous thresholds, the Government's National Cyber Security Strategy: 2022 to 2030, and the responses we received to our consultation.

3.27 As we also explained in the consultation, we maintain our opinion that these new thresholds will help to ensure that the performance of our general duties (within the meaning of section 3 of the Communications Act 2003) is secured or furthered by or in relation to what we have decided. In that regard, we set out our impact assessment in the consultation and we continue to believe that our expected increase in reporting (with associated costs) is both needed and proportionate, and that we consider that it would not be too burdensome for the OES to make such reporting to Ofcom.

3.28 In that regard, we set out our impact assessment in the consultation and we continue to believe that our expected increase in reporting (with associated costs) is both needed and proportionate, and that we consider that it would not be too burdensome for the OES to make such reporting to Ofcom.

3.29 We also do not consider that any of the decisions set out in this statement will have any equality impacts (whether in Northern Ireland or the rest of the UK). This is because we consider that they are likely to affect all citizens and consumers in the same way and would not have any particular implications for the different equality groups.

3.30 In reaching this decision, we have also had regard to the National Cyber Strategy 2022, and in particular, the three objectives of Pillar 2 (Building a resilient and prosperous digital UK).

Ofcom decision on updated referencing to our Enforcement Guidelines

3.31 Following on from our publication of Ofcom's Regulatory Enforcement Guidelines which now includes the relevant aspects of the NIS Regulations within its scope, we have decided to update the relevant section of the NIS Guidance accordingly, by removing the superseded content and replacing it with a reference to the 2022 Regulatory Enforcement Guidelines. We note that we received no stakeholder comments on this approach in response to the consultation.

Ofcom decision on other changes to our NIS Guidance

3.32 We have taken the opportunity presented by revising our NIS Guidance to make several other administrative updates. These include:

- replacing references to DCMS with DSIT – the current relevant Government department;
- noting changes to relevant sections of the Communications Act; and
- adding additional glossary entries.