making communications work
for everyone

Proposed changes to Ofcom’s NIS Guidance focusing on Incident Reporting Thresholds for the digital infrastructure subsector

Consultation on revising Ofcom’s NIS Guidance

CONSULTATION:

Publication date: 1 November 2022

Closing date for responses: 13 January 2023

Contents

Section

Annex

1. Overview

We are consulting on our proposed revisions to our incident reporting thresholds set out in Section 5 of our NIS Guidance.[1]

Ofcom is the designated competent authority for the digital infrastructure subsector in the United Kingdom (**"UK"**) under the Network and Information Systems Regulations 2018 (more commonly referred to simply as the **"NIS Regulations"**). In this role, we must prepare and publish statutory guidance in relation to that subsector under the NIS Regulations. In particular, we may publish guidance to deal with matters to which operators of essential services (**"OES"**) must have regard in complying with their security duties and also their separate duties to notify NIS incidents to Ofcom.

We last updated our NIS Guidance on 5 February 2021, but the existing incident reporting thresholds remain substantively unchanged since our Interim NIS Guidance from 8 May 2018. We are now proposing to amend our incident reporting thresholds, particularly in light of several incidents which occurred during 2020-2022. We believe these incidents could have had a significant impact on the continuity of essential services in our subsector, but we recognise that they fell below the existing reporting thresholds in our NIS Guidance.

What we are proposing – in brief

Lowering our incident reporting thresholds in our NIS Guidance. We are proposing to lower our incident reporting thresholds to better reflect our expectations of which incidents should be reported to us by OES, pursuant to their statutory duties under regulation 11(1). Improved visibility of incidents impacting UK users being reported to Ofcom will enable us to better understand causes of disruption to essential services, identify significant cyber security and resilience gaps and spot thematic trends across the digital infrastructure subsector. We will work with OES as they remediate any reported issues, with the aspiration that they are delivering an improved level of service to users of internet services across the UK.

Updating reference to our regulatory enforcement guidelines in our NIS Guidance. We are proposing to make reference to our revised Regulatory Enforcement Guidelines.

[1] '*Guidance for the digital infrastructure sector – Statutory guidance under the Network and Information Systems Regulations 2018: NIS Guidance*', as published by Ofcom on 5 February 2021, see: https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/guidance-network-information-systems-regulations

2. Introduction

Legal framework and our existing incident reporting thresholds

2.1 Before we set out our proposed new incident reporting thresholds in Section 3, it is important to put our incident reporting thresholds into their proper legal and regulatory context.

2.2 Regulation 11(1) of the NIS Regulations imposes a statutory duty on an 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"**). Our NIS Guidance[2] contains information about how OES must report NIS incidents to Ofcom, including our template NIS Incident Report form[3] together with associated guidance.

2.3 In determining the significance of the impact of an incident, regulation 11(2) of the NIS Regulations imposes a duty on an OES to have regard to the following three factors:

- the number of users affected by the disruption of the essential service;
- the duration of the incident; and
- the geographical area affected by the NIS incident.

2.4 Regulation 11(12) also requires an OES to have regard to any relevant guidance issued by the relevant competent authority (like Ofcom) when carrying out duties imposed on the OES by regulation 11(1) to (4).

2.5 We note that the regulations stipulate the three factors mentioned above to determine significance of an incident, but the regulations do not stipulate any specific metrics or thresholds for these factors. These metrics or thresholds have been provided by Ofcom as part of the duty under regulation 3(3)(b) of the NIS Regulations to prepare and publish statutory guidance in relation to the digital infrastructure subsector. This tries to ensure that OESs are measuring significant incidents consistently using service specific thresholds.

2.6 In other words, 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" on the continuity of the essential service which that OES provides by reference to the above-mentioned three factors laid down in regulation 11(2). As already noted above, 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 from time to time.

2.7 However, our incident reporting thresholds (see Table 1 below) utilise a broad proxy of metrics to measure and define an incident having a significant impact when they are met or exceeded. In particular, our thresholds signal to OES that, if we were to investigate any potential failure to notify an incident to us, we are likely to examine as our starting point whether our own thresholds were exceeded in relation to the incident in question.

[2] See paragraphs 5.15 to 5.20 of Ofcom's NIS Guidance.

[3] See Annex 2 to Ofcom's NIS Guidance.

Table 1: Ofcom's Existing Incident reporting thresholds within the NIS Guidance

Essential service for this subsector	Metric	Service Degradation
TLD Name Registry	Loss or significant degradation of >= 50% of aggregated name resolution capability (measured in queries per second)	1 hour
DNS Resolver Service	Loss or significant degradation of service to >= 50% of aggregated DNS Resolver capacity (measured in queries per second)	30 minutes
DNS Authoritative Hosting Service	Loss or significant degradation (e.g. serving incorrect results) of service for >=50% of registered domains	1 hour
IXP	Loss or significant degradation of connectivity to 25% of connected ASN; OR	1 hour
	Loss of >= 90% of total port capacity	

2.8 Our NIS Guidance makes it clear that, if the thresholds set out in Table 1 above are met or exceeded in relation to an essential service for the digital infrastructure subsector, the OES in question must report the incident to us as a NIS incident likely having a significant impact. We also note our expectation that any OES providing the essential services referred to in Table 1 above should not adopt an unduly restrictive approach to interpreting our thresholds. Our general guidance is that, if there is any doubt as to whether (or not) a threshold is met, an OES should take a cautious approach and submit an incident report to us on a fail-safe basis.

The Government's updated National Cyber Strategy 2022

2.9 We have considered that our proposed update to the NIS guidance enables us to factor in the recent publication of the Government's updated National Cyber Strategy 2022.

2.10 On 7 February 2022, the Government published its updated National Cyber Strategy 2022.[4] Regulation 3(6) of the NIS Regulations requires that Ofcom must have regard to the NIS National Strategy (which is annexed to the National Cyber Strategy 2022 document) when carrying out our duties under the NIS Regulations.

2.11 One of the matters that the National Cyber Strategy addresses is the regulatory measures and enforcement framework to secure the objectives and priorities of the strategy. The Strategy includes five pillars of priority actions to achieve certain intended outcomes by 2025. Pillar 2 (Building a resilient and prosperous digital UK) is particularly relevant to our

[4] https://www.gov.uk/government/publications/national-cyber-strategy-2022

review of the incident reporting thresholds. It is about reducing cyber risks so businesses can maximise the economic benefits of digital technology and citizens are more secure online and confident that their data is protected. It involves three objectives:

- improving the understanding of cyber risk to drive more effective action on cyber security and resilience.
- preventing and resisting cyber-attacks more effectively by improving management of cyber risk within UK organisations, and providing greater protection to citizens; and
- strengthening resilience at national and organisational level to prepare for, respond to and recover from cyber-attacks.

2.12 Achieving these objectives is something that we have considered in proposing our new incident reporting thresholds discussed in Section 3 of this consultation.

3. Our Incident Reporting Thresholds proposals

Practical approach to the three factors in regulation 11(2)

3.1 We have already explained in Section 2 of this 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.

3.2 Considering the nature of the digital infrastructure subsector, delivery of essential services to users within the UK often occurs with the OES not having a direct relationship with the users of the service, who are, in most cases, downstream of Public Electronic Communications Networks and Services (PECN and PECS). Thus, it may not be feasible for OES to determine the exact number of users impacted without undue delay and in any event no later than 72 hours after the operator is aware the incident occurring, which is the deadline imposed for reporting by regulation 11(3)(b) of the NIS Regulations.

3.3 For that reason, our existing incident reporting thresholds use various metrics as proxies to determine the number of users affected by the disruption of the essential service, in particular:

- for TLD Name Registry Services and DNS Resolver Services, the thresholds refer to the number of queries.
- for DNS Authoritative Hosting Services, the thresholds refer to registered domains; and
- for IXP Services, the thresholds refer to connected Autonomous System Number (ASNs) or ports.

3.4 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.

Overview of our proposed revised thresholds

3.5 Table 2 below gives an overview of our proposed new incident reporting thresholds, as compared to our existing thresholds.

3.6 We have outlined the reasons for our changes in the incident reporting thresholds in paragraph 3.25 below. These proposed thresholds will increase the number of incidents which are of significant impact being reported to Ofcom.

3.7 Based on our new proposals, an incident should be reported to Ofcom when both of the following conditions are satisfied[5]:

- a volume threshold is met or exceeded; and
- an outage duration is met.

3.8 We consider that a service degradation by volume of 25%, by time of 15 minutes or above will have significant impact and should be reported to Ofcom. Also, IXPs are now required to report incidents based on the loss of 50% of the total bandwidth capacity across all ports. A service degradation in all cases is proportionate and justifiable because, if such degradation were to occur, a potential large volume of users could be unable to get access to critical services such as healthcare, financial services, remote working, education, online shopping, certain communications, and collaboration platforms.

3.9 We discuss below our proposed new incident reporting thresholds for each of the essential services in the digital infrastructure subsector by giving some examples and by explaining the proxies we are proposing to use in relation to the three factors set out in regulation 11(2).

[5] Again, we remind OES in our digital infrastructure subsector that they are obliged themselves to consider the significance of any impact of an incident by reference to the three factors specified in regulation 11(2) of the NIS Regulations, irrespective of what our own incident reporting thresholds state from time to time.

Table 2: Summary of Existing Incident Reporting Thresholds and Ofcom’s Proposed New Thresholds

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

Proposed thresholds for TLD Name Registry Services

3.10 For the essential service of a TLD Name Registry, the threshold requirement[6] in the UK to be deemed as an OES under regulation 8(1) of the NIS Regulations is, irrespective of its place of establishment (whether within, or outside of, the United Kingdom), a TLD Name Registry which services 14 billion or more queries from any devices located within the UK in any consecutive 168-hour period for domains registered within the Internet Corporation for Assigned Names and Numbers (ICANN).

3.11 In light of that threshold requirement, Table 3 below sets out the proxies we are using in our proposed new incident reporting thresholds for TLD Name Registries in relation to the three factors set out in regulation 11(2).

3.12 By way of an example, let us assume that a TLD Name Registry (**"W"**) services 14 billion queries from devices located within the UK in any consecutive 168-hour period for a specific top-level domain registered with ICANN. In that case, W satisfies the above-mentioned threshold requirement. We assume that W is in scope for NIS and is deemed an OES according to the designation thresholds in the NIS regulations.

3.13 The 14 billion queries serviced by W's essential service equates to 2 billion per day on average. Furthermore, using our proposed service degradation metric of "a loss or significant degradation of >= 25% of aggregated name resolution capacity", this works out to a loss of up to 500 million queries a day (25% of 2 billion). Using this example, if an incident occurred resulting in the continuity of W's essential service being impacted for a period of 15 minutes, this will result in a loss of 5.21 million queries on average. Ofcom would consider this as a significant number of queries potentially impacting many users of critical/ essential services and warrants reporting.

Table 3: TLD Name Registry Service category

Essential service	Based on Regulation 11(2) factors	Comment
TLD Name Registry Service	**Number of users:** i. A user is a person who registers a domain name; and/or ii. A person or device who queries the registered domain.	Number of queries received are a proxy for number of users. The query resolution capacity of a TLD Name Registry is also a proxy for the number of users serviced by it. This is caveated as an approximation as a single user may generate multiple queries at any given time.
	Duration of incident	Numerical value (time) in hours and minutes.

[6] See paragraph 10(2) of Schedule 2 to the NIS Regulations.

	Geographical area	The general population would be affected by the loss or outage of a TLD. The impact area is the UK.

Proposed thresholds for DNS Resolver Services

3.14 For the essential service of a DNS resolver service provided by a DNS service provider, the threshold requirement[7] in the UK to be deemed as an OES under regulation 8(1) of the NIS Regulations is, irrespective of its place of establishment (whether within, or outside of, the UK), a DNS resolver service which services 500,000 or more different Internet Protocol addresses used by persons in the UK in any consecutive 168-hour period.

3.15 In light of that threshold requirement, Table 4 below explains the proxies we are using in our proposed new incident reporting thresholds for DNS resolver services in relation to the three factors set out in regulation 11(2).

3.16 As there is no direct proxy to end users in the case of DNS resolver services, because any user may be trying to query several different unique websites. That said, for the purpose of our new reporting thresholds, 25% loss of aggregated DNS resolver capacity could be equated to 100% of users of a particular DNS resolving service losing 25% DNS resolver capacity, i.e. all users using that particular DNS resolver service, would lose access to 25% of DNS resolving services. This could impact users by having either a total loss of internet access or significant service degradation including but not limited to access to various websites, internet applications: email, remote access/VPN, and other critical applications or services.

Table 4: DNS Resolver Service category

Essential service	Based on Regulation 11(2) factors	Comment
DNS Resolver Service	**Number of users:** i. A user is a person who uses an Internet protocol address; and/or ii. A person or device that queries an Internet protocol address.	The query resolution capacity of a DNS Resolver cannot be used as a proxy for users, but the market share of a specific public DNS resolver can aid in calculating percentage of users impacted.
	Duration	numerical value (time) in hours and minutes
	Geographical area	The impact area is nationwide (UK).

[7] See paragraph 10(3) of Schedule 2 to the NIS Regulations.

Proposed thresholds for DNS Authoritative Hosting Services

3.17 For the essential service of a DNS authoritative hosting service provided by a DNS service provider, the threshold requirement[8] in the UK to be deemed as an OES under regulation 8(1) of the NIS Regulations is, irrespective of its place of establishment (whether within, or outside of, the UK), a DNS authoritative hosting service which services 100,000 or more domains registered to persons with an address in the UK.

3.18 In light of that threshold requirement, Table 5 below explains the proxies we are using in our proposed new incident reporting thresholds for DNS Authoritative Hosting Services in relation to the three factors set out in regulation 11(2).

3.19 By way of an example, let us assume that a DNS authoritative hosting service provider (**"Y"**) services 100,000 or more domains registered to persons with UK addresses. In that case, Y satisfies the above-mentioned threshold requirement. We assume that Y is in scope for NIS and is deemed an OES according to the designation thresholds in the NIS regulations.

3.20 Using that example, suppose that an incident occurs as result of which the continuity of Y's essential service is affected for a period of 15 minutes, causing a Loss or significant degradation (e.g. serving incorrect results) of service for >=25% of registered domains. There is no direct link to the number of domains an Authoritative DNS Hosts and the impact of downtime to the number of users. At any given time, any UK user could be browsing a website or sending an email using domains registered to the authoritative host. Therefore a 15-minute outage of >=25% of total domains registered would result in all UK users being unable to access 25,000 websites and email domains. Ofcom considers this a significant number of websites or email domains potentially impacting a large number of users of critical/ essential services.

Table 5: DNS Authoritative Hosting Service category

Essential service	Based on Regulation 11(2) factors	Comment
DNS Authoritative Hosting Service	**Number of users:** A user is a person who accesses a registered domain for browsing or emailing or other related internet services.	The number of domains registered with the Authoritative host is a measure of capacity of a DNS Authoritative hosting service and has no direct equivalence to number of users. An outage of 25% DNS Authoritative Hosting capacity could have a UK wide impact to many users if any of those domains were related to Critical National Infrastructure (CNI) or other critical services like but not limited to online banking and NHS

[8] See paragraph 10(3A) of Schedule 2 to the NIS Regulations.

	Duration	numerical value (time) in hours and minutes
	Geographical area	UK

Proposed thresholds for IXP Services

3.21 For the essential service of an IXP provided by an IXP operator, the threshold requirement[9] in the UK to be deemed as an OES under regulation 8(1) of the NIS Regulations, irrespective of its place of establishment (whether within, or outside of, the UK), is an IXP operator which has 30% or more market share amongst IXP operators in the UK, in terms of interconnected autonomous systems.

3.22 In light of that threshold requirement, Table 6 below explains the proxies we are using in our proposed new incident reporting thresholds for Internet Exchange Point services in relation to the three factors set out in regulation 11(2).

3.23 The new thresholds set for IXP incidents using metrics of either loss or significant degradation of connectivity to >=25% of connected Autonomous System Numbers (ASN) or loss of >= 50% of total port capacity. It is important to understand that IXPs are essentially an interconnection point for multiple independent operators of networks (CPs) and large enterprises.

3.24 By way of an example, let us assume that a London based IXP operator (**"Z"**) services 1000 ASNs, via 500 ports, where an ASN (a unique identifier of an entity whose network is part of the internet). Using that example, suppose that an incident occurs as a result of which the continuity of Z's essential service is affected for a period of 15 minutes with a degradation of 25% of its ASN connectivity or loss of interconnections, causing a loss >=25% of connected ASN or 50% of total port capacity, this works out to a loss of 250 ASNs or 250 ports. Based on the example above, this could lead to significant impact to potentially the whole of the London area (with over 2million users) and nation which Ofcom considers is an incident with significant impact on a large number of users of critical/ essential services.

Table 6: IXP Service category

Essential service	Based on Regulation 11(2) factors	Comment
IXP Service	**Number of users**: A user is a person who accesses a network connected via an IXP via their ISP or enterprise	The number of users would be a conservative estimate based on the regional or national operations of the IXP by considering the population of that geography.

[9] See paragraph 10(4) of Schedule 2 to the NIS Regulations.

	Duration	numerical value (time) in hours and minutes
	Geographical area	It maybe regional or nationwide depending on the areas of operation i.e. an outage of the London hub may impact the global connections for all regional pops but an outage of the Manchester pop may only impact the Manchester region.

Our reasoning for our proposed new incident reporting thresholds

3.25 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.[10] 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 sub-sector 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

3.26 The internet relies on the optimal operation and availability of certain key 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).

3.27 The high dependency on digital infrastructure 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, and schooling and online educational content. These services now play a vital role in the functioning of the UK economy and they are important for overall societal wellbeing.

3.28 Critical services within other NIS sectors and CNI services are increasingly dependent on digital infrastructure services. They are adopting digital technologies or moving to the cloud. This move to 'digital' or cloud services means most of these sectors rely increasingly on applications which are cloud-based. For example, an incident in the digital infrastructure subsector can result in significant outages like loss of certain

[10] 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.

communications applications, loss of ticketing systems in the transportation sector or failure of safety systems which are cloud based.

3.29 Furthermore, communications providers[11] (**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[12].

3.30 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.

Lack of voluntary reports from OES

3.31 We have explained above the statutory duty on OES to report incidents to us, in particular that OES are obliged themselves to consider the significance of any impact of an incident by reference to the three factors specified in regulation 11(2) of the NIS Regulations.

3.32 In that regard, we also note that our NIS Guidance requests that OES report to us incidents that may not have met the incident reporting thresholds, but which had the potential to exceed a threshold. Such voluntary incident reporting would assist us in identifying thematic issues across the digital infrastructure subsector.[13]

3.33 Incident reports also serve as a mechanism for Ofcom to engage with OESs to identify issues and gaps against NIS regulatory duties of the OES. Working with the OESs we could look to understand the root causes and agree remediation plans to improve services.

3.34 Given that the incidents shown in Table 7 in Section 3 of this consultation were not reported to us, we consider that our approach to voluntary reporting has also proved ineffective and that it is necessary to revise our existing incident reporting thresholds.

[11] By CPs, we specifically refer to persons who provide an electronic communications network or an electronic communications service.

[12] https://inform.tmforum.org/future-oss-bss/2020/08/saas-the-new-revolution-in-telecom-bss/

[13] See paragraphs 5.31 to 5.34 of Ofcom's NIS Guidance.

Examples of outages reported in the media yet were unreported to Ofcom triggering our review of the current incident reporting thresholds

3.35 We are aware of several outages in the digital infrastructure subsector between 2020-2022 that were reported in the media, but predominantly not reported to Ofcom. We recognise that the impact of those outages did not meet our existing incident reporting thresholds set out in the NIS Guidance, which may be the reason why they were not considered significant and not reported to us. Table 7 below outlines examples of incidents which were reported by the media or organisations websites but remained unreported to Ofcom. The Ofcom' estimated impact of these incidents to users is based on our calculations (see Annex A4).

Table 7: Examples of incidents unreported to Ofcom between 2020-2022

DI Provider	Date	Service Degradation	Ofcom' Estimate of Impact to 'Number of Users' as per Ofcom's calculations (see Annex A4 on methodology)	Duration	Geography
A [14]	17 July 2020	50%	18.75 million	27 mins	UK wide
B [15]	18 August 2020	100%	8.28 million [16]	17h 19mins	Primarily London but UK wide impact to downstream dependencies
C [17]	23 March 2021	No data	No Data	13 mins	London
D [18]	23 March 2021	No data	No data	16 mins	London
E [19]	21 December 2021	10%	61.73 million. [20]	30 Mins	UK wide

[14] https://www.cloudflarestatus.com/incidents/b888fyhbygb8

[15] https://www.linx.net/incidents-log/

[16] This is based on population of London in 2020 at approx. 9million and ONS reporting 92% of UK population had access internet (https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2020#:~:text=1.,aged%2075%20years%20and%20over.)

[17] https://www.linx.net/incidents-log/

[18] https://www.linx.net/incidents-log/

[19] https://status.names.co.uk/incidents/8csdsj7qq5sf

[20] This incident impacted 10% of Namesco customers equating to over 200k emails domains and 190k web domains. User impact potentially would be anyone in the UK who tried to access affected web domains or email domains. Impact = UK population x percentage of users with internet access.

F[21]	5 November 2020	No data	61.73 million.[22]	6 days	UK wide

What our Estimated Impact to 'Number of Users' indicate

3.36 In light of the calculations in Annex A4 below, against existing thresholds (see Table 1 in Section 2 of this consultation), we note that these incidents could be considered significant yet remained predominantly unreported as they fell below the current incident reporting thresholds in our NIS guidance. Going forwards, we consider that such incidents could be considered as potentially having a significant impact on the continuity of the essential services and, as such, they should be reported to Ofcom.

Ofcom expectations on incident reporting thresholds

3.37 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).

3.38 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.

3.39 We note that, in complying with their security duties under regulation 10, all OES falling within the digital infrastructure subsector should already have tools and processes to monitor and log incidents that occur internally within their organisations. Those tools and processes should include the preparation of reports. Given that the incident reports[23] to be provided to Ofcom are brief and request for key information, we consider that our proposed new incident reporting thresholds are objectively justifiable and proportionate.

3.40 In proposing our new incident reporting thresholds, we have also taken into consideration the level of disruption to users which is likely to be the result for incidents exceeding our proposed thresholds, including on the wider economy and society as a whole such as:

- **Risks to the health and safety of the population:** An incident exceeding our proposed thresholds may have an impact on the health and safety of the population where critical services become unreachable due to a DNS outage, e.g. GP triage apps which provide a

[21] GoDaddy owned 123 Reg https://www.theregister.com/2020/11/11/123_reg/

[22] This incident impacted 123 Reg domains of which their website claims they manage over 1 million UK websites which could equate to UK wide users unable to access a large number of UK websites

[23] See, in particular, Annex 2 to our NIS Guidance, which sets out our template for the incident report form.

quick and safe means of medical consultation (like Klinik and PATCHS, email, video consultation) and certain 111 services.

- **Damages and costs for users and/or organizations affected:** DNS-related outages can be very expensive for users and organisations. It was reported in the media that just one hour of downtime can cost a business as much as £540,000[24] or more, depending on the size of the organisation. The scope of loss is potentially greater than just what happens during an outage. Staff costs and loss of productivity are other considerations to factor in. Not only do IT departments have to work to fix any outage-related issues during and after an event, but productivity may also fall company-wide when employees are not able to access systems or online platforms, they need to do their jobs.
- **Disruption to daily life:** Reports show that 98% of the UK population[25] uses the internet and an outage will disrupt the activities and lives of the population who rely on the internet to carry out essential activities like working from home, education, banking and other economic activities.
- **Cascading effects in other critical sectors**: According to the NCSC[26], the critical national infrastructure (CNI) is becoming increasingly dependent on our digital infrastructure. As such, there is an increase in interdependency between other NIS sectors and the digital infrastructure. E.g. the transportation sector delivers services which would potentially be adversely impacted if digital infrastructure services suffered significant outages like loss of communication, loss of ticketing systems or failure of safety systems. Many sectors are also seeing digitisation blurring the lines between Information Technology (IT) and Operational Technology (OT) which were traditionally separate from the internet, however, with the introduction of Internet of Things (IoT) devices there is an absolute need for connectivity to the internet.
- **Government digital services impact and significance:** CNI and general services across both central and local governments which have been digitized, would also be impacted by outages of digital infrastructure e.g. HMRC, website for tax returns, DVLA, MOT/ Road tax, Council tax, claiming benefits etc. In considering our proposal to reduce the incident reporting thresholds, we have had regard to the Government's National Cyber Strategy 2022 (as discussed in Section 2 of this consultation).

3.41 Overall, we also consider that our proposed thresholds would further the interests of Citizens and consumers in accordance with our general duties under section 3 of the Communications Act 2002 (**"CA 2003"**). In addition, we have also taken into account our approach to voluntary reporting in the NIS Guidance which has proved to be ineffective in relation to the unreported incidents discussed in Section 2 of this consultation.

[24] https://constellix.com/news/dns-server-widespread-outages-need-for-redundancy

[25] https://datareportal.com/reports/digital-2022-united-kingdom#:~:text=There%20were%2066.99%20million%20internet,percent)%20between%202021%20and%202022

[26] https://www.ncsc.gov.uk/section/private-sector-cni/cni

4. Updated reference to Regulatory Enforcement Guidelines

Our approach to enforcement

4.1 Section 9 of the NIS Guidance sets out how we would normally approach enforcement action in cases relating to relevant failures to comply with relevant requirements of the NIS Regulations, together with our imposition of any penalties on OES.

4.2 In particular, we explain in that Section 9 that we would normally expect that our approach to enforcement of the NIS Regulations to be broadly in line with the approach we take in cases relating to electronic communications networks and services, postal services and some cases relating to breaches of wireless telegraphy licences, as set out in our Enforcement Guidelines for regulatory investigations published on 28 June 2017 (the **"Regulatory Enforcement Guidelines"**).

4.3 On 24 May 2022, we published a consultation on revising the Regulatory Enforcement Guidelines[27]. One of the proposals in that consultation is to set out our expected enforcement approach in relation to network security, including compliance with requirements on OES under the NIS Regulations. That specific proposal is dealt with in Annex 3 of the draft guidelines for consultation.[28]

4.4 Accordingly, if we decide to adopt those draft Guidelines, we intend to update our NIS Guidance by simply cross-referring in Section 9 of the NIS Guidance to the revised Regulatory Enforcement Guidelines and delete the remainder of that Section 9.

General impact assessment

4.5 Impact assessments provide a valuable way of assessing different options for regulation and showing why the preferred option was chosen. They form part of best practice policymaking. This is reflected in section 7 of the CA 2003, which means that generally Ofcom must carry out impact assessments where its proposals would be likely to have a significant effect on businesses or the general public, or when there is a major change in Ofcom's activities. However, as a matter of policy, Ofcom is committed to carrying out and publishing impact assessments in relation to the vast majority of its policy decisions.

4.6 For further information about Ofcom's approach to impact assessments, see our guidelines, 'Better policy-making: Ofcom's approach to Impact Assessment'.[29] Specifically, pursuant to section 7, an impact assessment must set out how, in our opinion, the

[27] '*Ofcom's approach to enforcement – Consultation on revising the Regulatory Enforcement Guidelines*', as published on 24 May 2022, see: https://www.ofcom.org.uk/consultations-and-statements/category-2/revising-regulatory-enforcement-guidelines

[28] See: https://www.ofcom.org.uk/__data/assets/pdf_file/0023/238046/draft-revised-enforcement-guidelines.pdf

[29] https://www.ofcom.org.uk/about-ofcom/policies-and-guidelines.

performance of our general duties (within the meaning of section 3 of the CA 2003) is secured or furthered by or in relation to what we propose.

4.7 The analysis presented in the entirety of this consultation represents an impact assessment. As already explained above, we are proposing, in effect, to lower our incident reporting thresholds set out in the NIS Guidance. We therefore expect that our new thresholds would result in an increase in incidents reported to us going forwards. We broadly estimate an increase in reported incidents by around 50%, based on historical incidents which would now fall within our new proposed reporting thresholds, if we were to decide to adopt them and OES were then to follow our guidance in that regard.

4.8 If so, such an increase in reporting would have an impact on OESs. That burden, together with associated costs, on OES to submit incident reports to us in the form and manner set out in our NIS Guidance would increase. Such increased reporting would also have an impact on Ofcom by us handling, reviewing and following up more reported incidents. This is likely to increase our own administrative costs in dealing with such matters.

4.9 However, as discussed above, the duty on OES to notify incidents to Ofcom stems from regulation 11(1) of the NIS Regulations, including the three factors specified in regulation 11(2), and not our NIS Guidance alone. We have also set out our view above why we consider that such an increase in reporting (with associated cost) is needed and proportionate, and the reasons why we consider it would not be too burdensome for the OES.

Equality impact assessment

4.10 We have considered whether our proposed new incident reporting thresholds will have a particular impact on persons sharing protected characteristics (broadly including race, age, disability, sex, sexual orientation, gender reassignment, pregnancy and maternity, marriage and civil partnership and religion or belief in the UK and also dependents and political opinion in Northern Ireland), and in particular whether they may discriminate against such persons or impact on equality of opportunity or good relations. This assessment helps us comply with our duties under section 149 of the Equality Act 2010 and section 75 of the Northern Ireland Act 1998.

4.11 We do not consider that any of the proposals on which we are consulting will have any equality impacts (whether in Northern Ireland or the rest of the UK). This is because we consider that the proposals in this document are likely to affect all citizens and consumers in the same way and would not have any particular implications for the different equality groups.

Next steps

4.12 We are consulting for 10 weeks on our proposed new incident reporting thresholds. Ofcom therefore invites responses to this consultation by 13 January 2023. Details on how to respond to Ofcom are set out in Annex A1.

4.13 After considering the responses, we plan to issue our final statement and our final guidance in Spring 2023.

A1. Responding to this consultation

How to respond

A1.1 Ofcom would like to receive views and comments on the issues raised in this document, by 5pm on 13 January 2023.

A1.2 You can download a response form from https://www.ofcom.org.uk/consultations-and-statements/category-1/proposed-changes-to-nis-guidance-incident-reporting-thresholds. You can return this by email or post to the address provided in the response form.

A1.3 If your response is a large file, or has supporting charts, tables or other data, please email it to nisconsultation@ofcom.org.uk, as an attachment in Microsoft Word format, together with the cover sheet. This email address is for this consultation only and will not be valid after 13 January 2023.

Responses may alternatively be posted to the address below, marked with the title of the consultation:

NIS Consultation
Network Security Team
Networks & Communications Group
The Office of Communications
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

A1.4 We welcome responses in formats other than print, for example an audio recording or a British Sign Language video. To respond in BSL:

- send us a recording of you signing your response. This should be no longer than 5 minutes. Suitable file formats are DVDs, wmv or QuickTime files; or
- upload a video of you signing your response directly to YouTube (or another hosting site) and send us the link.

A1.5 We will publish a transcript of any audio or video responses we receive (unless your response is confidential)

A1.6 We do not need a paper copy of your response as well as an electronic version. We will acknowledge receipt of a response submitted to us by email.

A1.7 You do not have to answer all the questions in the consultation if you do not have a view; a short response on just one point is fine. We also welcome joint responses.

A1.8 It would be helpful if your response could include direct answers to the questions asked in the consultation document. The questions are listed here. It would also help if you could explain why you hold your views, and what you think the effect of Ofcom's proposals would be.

A1.9 If you want to discuss the issues and questions raised in this consultation, please contact Onome Anirah on 02077834240, or by email to nisconsultation@ofcom.org.uk

Confidentiality

A1.10 Consultations are more effective if we publish the responses before the consultation period closes. In particular, this can help people and organisations with limited resources or familiarity with the issues to respond in a more informed way. So, in the interests of transparency and good regulatory practice, and because we believe it is important that everyone who is interested in an issue can see other respondents' views, we usually publish responses on the Ofcom website at regular intervals during and after the consultation period.

A1.11 If you think your response should be kept confidential, please specify which part(s) this applies to and explain why. Please send any confidential sections as a separate annex. If you want your name, address, other contact details or job title to remain confidential, please provide them only in the cover sheet, so that we don't have to edit your response.

A1.12 If someone asks us to keep part or all of a response confidential, we will treat this request seriously and try to respect it. But sometimes we will need to publish all responses, including those that are marked as confidential, in order to meet legal obligations.

A1.13 To fulfil our pre-disclosure duty, we may share a copy of your response with the relevant government department before we publish it on our website. This is the Department for Business, Energy and Industrial Strategy (BEIS) for postal matters, and the Department for Culture, Media and Sport (DCMS) for all other matters.

A1.14 Please also note that copyright and all other intellectual property in responses will be assumed to be licensed to Ofcom to use. Ofcom's intellectual property rights are explained further in our Terms of Use.

Next steps

A1.15 Following this consultation period, Ofcom plans to publish a statement in Spring 2023.

A1.16 If you wish, you can register to receive mail updates alerting you to new Ofcom publications.

Ofcom's consultation processes

A1.17 Ofcom aims to make responding to a consultation as easy as possible. For more information, please see our consultation principles in Annex A2.

A1.18 If you have any comments or suggestions on how we manage our consultations, please email us at consult@ofcom.org.uk. We particularly welcome ideas on how Ofcom could more effectively seek the views of groups or individuals, such as small businesses and residential consumers, who are less likely to give their opinions through a formal consultation.

A1.19 If you would like to discuss these issues, or Ofcom's consultation processes more generally, please contact the corporation secretary:

Corporation Secretary
Ofcom
Riverside House
2a Southwark Bridge Road
London SE1 9HA
Email: corporationsecretary@ofcom.org.uk

A2. Ofcom’s consultation principles

Ofcom has seven principles that it follows for every public written consultation:

Before the consultation

A2.1 Wherever possible, we will hold informal talks with people and organisations before announcing a big consultation, to find out whether we are thinking along the right lines. If we do not have enough time to do this, we will hold an open meeting to explain our proposals, shortly after announcing the consultation.

During the consultation

A2.2 We will be clear about whom we are consulting, why, on what questions and for how long.

A2.3 We will make the consultation document as short and simple as possible, with an overview of no more than two pages. We will try to make it as easy as possible for people to give us a written response.

A2.4 We will consult for up to ten weeks, depending on the potential impact of our proposals.

A2.5 A person within Ofcom will be in charge of making sure we follow our own guidelines and aim to reach the largest possible number of people and organisations who may be interested in the outcome of our decisions. Ofcom’s Consultation Champion is the main person to contact if you have views on the way we run our consultations.

A2.6 If we are not able to follow any of these seven principles, we will explain why.

After the consultation

A2.7 We think it is important that everyone who is interested in an issue can see other people’s views, so we usually publish the responses on our website at regular intervals during and after the consultation period. After the consultation we will make our decisions and publish a statement explaining what we are going to do, and why, showing how respondents’ views helped to shape these decisions.

A3. Consultation coversheet

BASIC DETAILS

Consultation title:

To (Ofcom contact):

Name of respondent:

Representing (self or organisation/s):

Address (if not received by email):

CONFIDENTIALITY

Please tick below what part of your response you consider is confidential, giving your reasons why

Nothing □

Name/contact details/job title □

Whole response □

Organisation □

Part of the response □

If there is no separate annex, which parts? ____

____

If you want part of your response, your name or your organisation not to be published, can Ofcom still publish a reference to the contents of your response (including, for any confidential parts, a general summary that does not disclose the specific information or enable you to be identified)?

DECLARATION

I confirm that the correspondence supplied with this cover sheet is a formal consultation response that Ofcom can publish. However, in supplying this response, I understand that Ofcom may need to publish all responses, including those which are marked as confidential, in order to meet legal obligations. If I have sent my response by email, Ofcom can disregard any standard e-mail text about not disclosing email contents and attachments.

Ofcom aims to publish responses at regular intervals during and after the consultation period. If your response is non-confidential (in whole or in part), and you would prefer us to publish your response only once the consultation has ended, please tick here.

Name Signed (if hard copy)

A4. Ofcom's calculations for the estimated level of impact to users during an incident

Our calculations below are estimated utilising the NIS designation thresholds in Regulation 8(1) for each NIS service category, against the existing Incident Reporting Thresholds.

A4.1 We explain below the magnitude of impact an incident could have on end users of essential services provided by OES in the digital infrastructure subsector. The estimates are reached using the NIS designation thresholds as measure of significant impact, in the calculations of number of users or geographical impact. This has provided the methodology for our estimated impact against the predominantly unreported incidents in Table 7.

SERVICE CATEGORY: TLD Name Registry Services

A4.2 Using the NIS OES designation thresholds for TLDs (14 billion queries in 168-hour period), as a baseline to determine a significant impact, an incident which had a 50% service degradation of DNS TLD services for 60 minutes would impact at least 41.66million queries. Queries here are used as a proxy for the approximate number of users potentially impacted but does not equate to a 1:1 mapping of users as a single user could generate multiple queries.

SERVICE CATEGORY: DNS Resolver Services

A4.3 There is no direct proxy to end users in the case of DNS Resolver Services, because any user may be trying to query several different unique websites or internet-based services like email. That said, for the purpose of our current reporting thresholds, 50% of aggregated DNS resolver capacity could be equated to 100% of users losing 50% DNS resolver capacity, i.e. all users using the particular DNS resolver service, would lose access to 50% of DNS resolving services.

A4.4 Based on a ICAAN report[30] on public DNS resolver uptake across the EU, it shows an average of 12.2% of EU users used a public DNS service. For the UK, that figure would equate to 7.57million users of DNS resolving services. To clarify, a 50% outage of DNS resolver capacity could impact a significant number of users (depending on market share of an OES public DNS resolver service this could range from 143,000 to 700,000 users) across the UK with potential for delayed or failed DNS resolutions equating to loss of access to internet services including browsing and email.

[30] UK population as of 2020: https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/bulletins/annualmidyearpopulationestimates/mid2020
Percentage of UK users using public DNS resolvers: https://www.icann.org/en/system/files/files/octo-032-01mar22-en.pdf
Percentage of UK population with internet access: https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2020

SERVICE CATEGORY: DNS Authoritative Hosting Services

A4.5 The number of users of DNS Authoritative Hosting Services cannot be directly measured with regard to the impact to users, because an OES may host 100,000 domains of which at any time any number of UK users may be accessing websites or email associated with those 100,000 domains.

A4.6 Our current threshold of loss or degradation to 50% of registered domains equates to 50,000 domains.

SERVICE CATEGORY: IXP Services

A4.7 The link to user impact from an incident for an IXP is difficult to establish as most IXP customers are CPs who would typically have redundancies (direct peer to peer interconnections or alternate IXP interconnections). However, based on a some of the outages we have observed with IXPs and a conservative estimate of IXP geographical impact using London as an example, we can see potential user impact could be as high as 2.07million users[31]. This is assuming the existing threshold metric of 25% degradation to IXP's interconnections measured by percentage of connected Autonomous System Numbers (ASN) which we have left unchanged.

[31] Calculation based on the population of London in 2020 at approx. 9million and ONS reporting 92% of UK population had access internet thus 50% degradation could result in 2.07million users being impacted

A5. Consultation questions

Questions concerning Ofcom's draft general statement on the updates to the NIS Guidance

Question 1: Do you agree or disagree with our proposed new incident reporting thresholds? Please set out your reasons, with supporting evidence, for your response.

Question 2: Do you have any other comments on our proposed new incident reporting thresholds?