Decision

Decision on Ofgem's proposed new NIS Enforcement Guidelines and Penalty Policy

Publication date:	1 December 2022
Response deadline:	30 November 2021
Contact:	Bruno Sheldon, Senior Manager
Team:	Enforcement
Telephone:	020 7901 7295
Email:	enforcement@ofgem.gov.uk

This document sets out the Gas and Electricity Markets Authority's ("the Authority") revisions to the NIS Enforcement Guidelines and Penalty Policy following our consultation, which ran from 4 October 2021 to 30 November 2021. Having considered stakeholder feedback, we have decided to publish the NIS Guidelines and Penalty Policy with some amendments. This document describes the key feedback themes and sets out our reasons for either making amendments or retaining the original text.

Any enquiries related to the text of this publication should be sent to Ofgem at:

10 South Colonnade, Canary Wharf, London, E14 4PU.

This publication is available at www.ofgem.gov.uk. Any enquiries regarding the use and re-use of this information resource should be sent to: psi@nationalarchives.gsi.gov.uk

Contents

Decision on Ofgem's proposed new NIS Enforcement Guidelines and Penalty Policy 1

Introduction 4

1. The proposed NIS Enforcement Guidelines 6

Stakeholder feedback from the consultation 6

Inspections 7

Information Notices 10

Decision-making arrangements 12

Overlap and consistency 12

Opening a case 14

Publication of case information 17

Other responses 17

2. The proposed NIS Penalty Policy 19

Stakeholder feedback from the consultation 19

3. Conclusion and next steps 23

Conclusion 23

Introduction

Context and related publications

The aim of the Network and Information Systems Regulations 2018 (NIS Regulations) are to drive improvement in the protection of the network and information systems that are critical for the delivery of the UK's essential services.

Designated operators of essential services (OES) must comply with duties set out in the NIS Regulations. These include taking 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.

Ofgem acting jointly with the Secretary of State for Business, Energy and Industrial Strategy (BEIS) is the competent authority (CA) responsible for regulating the activities of OES in the downstream gas and electricity sectors[1] (DGE) in England, Wales and Scotland.

The aim of Ofgem's NIS Enforcement Guidelines and Penalty Policy is to provide greater clarity, consistency and transparency to our enforcement policies and processes, and to describe the framework we have in place to maximise the impact and efficiency of our enforcement work under the NIS regime.

Ofgem has also published its updated NIS Guidance for Operators of Essential Services in Great Britain.[2] BEIS has published its updated Policy Guidance for the Implementation of the Network and Information Systems Regulations for the Energy Sector in Great Britain,[3] which includes sections on enforcement for which BEIS will be responsible.

[1] The relevant subsectors are (for electricity) those described in paragraph 1 of Schedule 2 to the NIS Regulations and (for gas) those described in paragraph 3 of Schedule 2 to the NIS Regulations, except for sub-paragraphs (5) to (8).
[2] https://www.ofgem.gov.uk/publications/nis-directive-and-nis-regulations-2018-ofgem-guidance-operators-essential-services
[3] https://www.gov.uk/government/publications/security-of-network-and-information-systems-regulation-2018-implementation-in-the-energy-sector-for-great-britain

Our decision-making process

A total of 10 responses were received from OES and other stakeholders.

We have considered the responses carefully before making decisions on the proposals and whether to make any amendments.

The first version of the NIS Enforcement Guidelines and Penalty Policy is published alongside this decision document. The Penalty Policy is annexed to the main guidelines document.

Decision-making stages

Date	**Stage description**
04/10/2021	Stage 1: Consultation open
30/11/2021	Stage 2: Consultation closes (awaiting decision), deadline for responses
01/12/2021	Stage 3: Responses reviewed
30/11/2022	Stage 4: Consultation decision/policy statement

General feedback

We believe that consultation is at the heart of good policy development. We are keen to receive your comments about this report. We'd also like to get your answers to these questions:

1. Do you have any comments about the overall quality of this document?
2. Do you have any comments about its tone and content?
3. Was it easy to read and understand? Or could it have been better written?
4. Are its conclusions balanced?
5. Did it make reasoned recommendations?
6. Any further comments?

Please send any general feedback comments to enforcement@ofgem.gov.uk.

1. The proposed NIS Enforcement Guidelines

Section summary

This section summarises the consultation responses to the first question in our consultation (shown below) and sets out our responses, including our reasons for deciding to make appropriate changes or retain the original text. The main themes emerging from the consultation responses were Inspections, Information Notices, decision-making arrangements and potential issues of overlap and consistency with other regulators, regimes, or guidance.

Question 1: With respect to the NIS Enforcement Guidelines, are the enforcement procedures for the DGE subsector clearly presented? We invite respondents' views on any aspect of the draft guidelines, including any suggestions for changes or additions.

Stakeholder feedback from the consultation

1.1 Stakeholders were broadly supportive of the new NIS Enforcement Guidelines. They believed the Guidelines would help improve clarity and transparency around Ofgem's NIS enforcement process.

1.2 However, some themes emerged from the consultation responses, which can broadly be characterised as requests for further information and clarity. Other responses that did not relate to one of the themes discussed below are documented and addressed under the sub-section titled "Other responses".

1.3 Please note that the paragraph numbers quoted below, which refer to consultation responses (rather than our response to them), are provided in reference to the draft version of the NIS Enforcement Guidelines, which was the subject of the consultation. Some of the relevant paragraph numbers may have changed in the final published version. We indicate where paragraph numbers have changed between the draft and final version of the document.

Inspections

1.4 Many responses were received regarding the sub-section titled "Power to inspect" (paragraphs 2.12 - 2.22) in Section 2 of the draft Guidelines.

1.5 Some highlighted concerns about paragraph 2.18, which sets out powers that an inspector has under the NIS Regulations. Respondents believed there was a potential conflict between inspectors having powers to require OES to preserve evidence (or being able to examine, copy or remove information and equipment) and the primary objective of securing and restoring service in the event of a cyber incident. Respondents stated containing incidents or restoring service might, for example, involve shutting down systems or overwriting data. Any direction to preserve data in such a circumstance could delay service restoration and increase security risk.

1.6 Some respondents referred to an inspector's power to conduct or direct an OES to conduct tests.[4] Respondents asked for clarification or for the power to be defined and reduced in scope or removed altogether.

1.7 Some also commented on potential unannounced, "on the spot inspections" (paragraph 2.17), or those conducted at short notice. Respondents considered that such inspections could be disruptive at critical phases of incident response. Again, respondents believed restoring service should be prioritised and that advance notice of inspections was important to ensure safety and security. One respondent asked for the term "reasonable grounds" (paragraph 2.16) to be further explained while another believed that OES should be given time to take legal advice in certain circumstances before inspectors could be granted access to sites, equipment, or information.

1.8 Regarding the inspectors themselves, some respondents asked for further information such as a published list or some means of reassuring OES that they were suitably qualified, experienced, and independent. Some respondents wanted reassurance on matters such as suitable confidentiality and security arrangements being in place before inspections could occur. Also, some

[4] Regulation 16(5)(f) of the NIS Regulations.

respondents believed there should be suitable means for ensuring the identity of inspectors before they could enter premises.

1.9 Some respondents challenged the first bullet point of paragraph 2.21, which states that OES are required to "pay the reasonable costs of inspection, if so required by us". One respondent believed that it was unreasonable to require OES to meet these costs while others asked for greater clarity on the meaning of "reasonable costs" in this context and how OES might be able to challenge costs. Another respondent asked for more clarity on how Ofgem would seek to keep costs under control.

1.10 One respondent believed that suspected non-compliance should be a pre-requisite of inspections carried out for compliance or enforcement purposes.

Ofgem response

1.11 Section 2 of the Guidelines is intended to set out Ofgem's powers under the NIS Regulations; in large part it articulates the regulations themselves. In that context, we consider that many of the relevant consultation responses amounted to questions about the NIS Regulations themselves, rather than the content of the Guidelines per se. On the matter of clarifying that a suspicion of non-compliance is a necessary pre-requisite for compliance or enforcement focussed inspections, we consider it may sometimes be the case in practice. However, there are other circumstances in which such inspections may be used; for example, to help determine that an OES is compliant having undertaken remedial action.

1.12 Regarding paragraph 2.18, we note the concerns of respondents but would point out that the NIS Regulations contain appropriate checks and balances. For example, Regulation 16(7)(a) requires that, before exercising certain powers, inspectors "must take such measures as appear to the inspector appropriate and proportionate to ensure that the ability of the OES […]to comply with any duty set out in these regulations will not be affected". Where this applies, inspectors would generally therefore take account of an OES's ability to meet its security duties under Regulation 10(2). The NIS Regulations are also clear that, before

exercising certain powers, an inspector may consult such persons as appear appropriate to them for the purpose of ascertaining any risks.[5]

1.13 With reference to an inspector's power to conduct or direct an OES to conduct tests,[6] again, the relevant text in the Guidelines document re-states CA powers as set out in the regulations themselves.

1.14 Regarding responses about the potential for "on the spot", or short notice inspections, the Guidelines indicate we will normally provide at least 48 hours' notice where it is appropriate and practicable to do so. Anything less than 48 hours would generally be reserved for "exceptional circumstances".[7] It is also worth noting the relevant footnote, which clarifies that inspectors will have regard to the Home Office Code of Practice on Powers of Entry where appropriate when exercising any functions to which the Code of Practice relates. In terms of security concerns about inspectors and any issues about interference with OES's ability to undertake their NIS duties, we consider there are appropriate checks and balances in the NIS Regulations. Regulations 16(6) and 16(7) place various requirements on inspectors such as presenting ID at premises on request, keeping evidence secure and, as noted above, in relation to allowing OES to comply with their duties. The relevant paragraphs in the Guidelines are re-statements of these checks and balances.

1.15 Considering concerns raised around inspections and inspectors, we have introduced new text at paragraphs 2.15 and 2.20 (previously paragraph 2.19) together with a new paragraph 2.16. The new text recommends that OES inform Ofgem, at the earliest opportunity, of any concerns about inspectors or the impact of a proposed compliance / enforcement inspection such that they are considered and resolved in advance wherever possible. We have also made minor cosmetic changes in paragraphs 2.13, 2.14, 2.19 and 2.21.

1.16 On the suitability of the inspectors themselves, we note that the NIS Regulations allow for CAs to conduct inspections, appoint an inspector, or direct an OES to appoint an inspector approved by us to carry out an inspection on our behalf. In paragraph 1.19 of the Guidelines, as part of the "Vision for our enforcement

[5] Regulation 16(7)(b) of the NIS Regulations.
[6] Regulation 16(5)(f) of the NIS Regulations.
[7] Regulation 11(5)(a) of the NIS Regulations

work" we state that we aim to be "fair" in the actions we take. Our inspectors, or those we appoint, are suitably qualified and experienced. For example, we generally seek to appoint suitably senior people with industry specific qualifications and experience in IT and cyber security and in inspecting or auditing (preferably in the DGE sector). We also seek to mix and match our inspection teams to ensure the best spread of knowledge and experience. We note there is no requirement in the NIS Regulations for inspectors to be "independent"; they will normally work for or on Ofgem's behalf.

1.17 Similar logic applies to the costs of inspections; the NIS Regulations require that OES "pay the reasonable costs of inspection" if required by the CA[8]. Again, Ofgem will seek to be reasonable in its approach to costs and any costs recovered must be reasonable under the NIS Regulations as set out above. To date Ofgem has not sought recovery of inspection costs. Our position in relation to inspection costs may change in the future and we will advise OES of any changes where appropriate.

1.18 In terms of defining what is meant by "reasonable" and having a means of challenging costs, the NIS Regulations do not include these elements. We appreciate these points and will consider them further, as appropriate. In practice, in an enforcement context it would be open to OES to query costs with Ofgem via usual feedback channels and we would consider such matters on a case-by-case basis, in line with our stated enforcement aim of being fair in our dealings with investigated parties.

Information Notices

1.19 Several respondents referred to the sub section titled "Power to serve an Information Notice" set out in paragraphs 2.2 – 2.11.

1.20 Various points were made about the process before the Information Notice was served. Respondents mentioned potentially needing to negotiate deadlines in advance and the need to be pragmatic when a live event was occurring (which should take priority they believed). One respondent said Ofgem should commit to sharing a draft of any Information Notice in advance unless there was a good

[8] Regulation 16(3) of the NIS Regulations.

reason not to. Another respondent believed there should be a formalised process written into the Guidelines explaining the steps that would be taken before any Information Notice was served. In reference to paragraph 2.11, a respondent stated Ofgem should provide reasons for withdrawing an Information Notice. With reference to the bullets in paragraph 2.4, one respondent suggested that further bullets could be added to clarify scope, particularly in relation to OES assessment in accordance with the Cyber Assessment Framework (CAF).

1.21 One respondent believed that requirements for OES to report or share information should be proportionate and focus on only essential information; requests for information should not unnecessarily burden OES and confidentiality should be preserved wherever possible.

Ofgem response

1.22 We consider that the Guidelines contain suitable language, which should allay concerns about unnecessary or burdensome information collection. The Guidelines are reflective of the provisions of the NIS Regulations and make clear that we will use our powers where appropriate to collect information "we reasonably require". In paragraph 2.6 we state that we will provide our reasons for requesting information as required under the NIS Regulations.

1.23 Regarding sharing copies of Information Notices in advance and timelines for response, we consider no changes to the Guidelines are necessary. In practice we are likely to share draft versions in advance where this would be helpful or appropriate, but we believe the "we may" qualification in paragraph 2.7 is sufficient; there may be circumstances in which sharing a draft in advance is not necessary, such as when the Notice is simple or short. As far as timelines are concerned, again, we consider that the text is suitably drafted. We state we will set deadlines taking into account matters such as complexity. Paragraph 2.6 states we will set reasonable deadlines "in the circumstances"; those circumstances could include when an OES needs to give priority to, for example, incident management.

1.24 We note there is no requirement in the NIS Regulations for CAs to provide OES with reasons for withdrawing an Information Notice. We consider that withdrawing an Information Notice is unlikely in any event and that if it were to happen, an OES would be free to request details of our reasons if needed and we

would generally provide these assuming that was necessary or appropriate in the circumstances.

Decision-making arrangements

1.25 In relation to decision-making arrangements for case opening, Enforcement Notices and Penalty Notices (paragraphs 3.38-3.40; 5.10-5.12; 6.10), one respondent queried why the proposed process might not require Enforcement Oversight Board (EOB) or Enforcement Decision Panel (EDP) oversight for certain cases; the respondent believed greater clarity was needed.

Ofgem response

1.26 We consider the NIS enforcement decision-making arrangements are reasonable and proportionate, striking the correct balance between the need for operational efficiency and more separation between the investigation and decision-making functions where that may be appropriate.

1.27 In practice the senior civil servant with responsibility for enforcement will normally take case opening decisions following a discussion with Ofgem's EOB. The EOB comprises several senior Ofgem employees from different policy areas whose role is (among other things) to help consider proposals made by the case investigation team at key stages of the case.

1.28 For Enforcement Notice and Penalty Notice decisions, the senior civil servant with responsibility for enforcement matters (or other appropriate decision-maker) will also usually act as a decision "gatekeeper" and may discuss with the EOB how decisions should be taken. The discussion will consider whether matters should be referred to our EDP for a decision. EDP members are specialist regulatory decision-makers employed specifically for EDP duties and work separately from the case team.

Overlap and consistency

1.29 Some of the responses asked for greater clarification on matters of potential overlap and consistency between CAs or different enforcement bodies.

1.30 One respondent believed that a lead CA should be identified for those OES that operate across multiple sectors. There was potential for confusion and overlap should more than one CA be regulating the same entity. The same respondent,

alongside another, believed there was potential for better international consistency, given that they would be regulated in different national jurisdictions.

1.31 A respondent expressed concerns about potential inconsistency with upcoming BEIS guidance and asked for further clarification on the distinction between the BEIS and Ofgem CA roles. Similarly, on the matter of publishing information, the respondent requested more clarity on how decisions would be handled and remain consistent between Ofgem and BEIS. Considering these concerns, the respondent requested another opportunity to review and comment on near final versions of the Ofgem and BEIS guidance.

1.32 More than one respondent expressed concern about potential increased burdens of any duplicative reporting requirements or overlaps or inconsistencies between enforcement regimes or assessment approaches. One respondent believed, for example, there could be duplication between CAF reporting requirements and others that Ofgem might impose via guidance.

Ofgem response

1.33 Ofgem has liaised closely with BEIS to ensure consistency across the various guidance being developed and to ensure that the roles are clearly defined and communicated. We have worked to ensure consistency while removing unnecessary duplication. We will continue to engage closely with BEIS to address any new concerns that may arise.

1.34 With that aim in mind, we have added a table to Section 1 of the Guidelines that sets out the roles of BEIS and Ofgem. The table should help clarify roles and responsibilities and ensure consistency across guidance.

1.35 In terms of the consistency of enforcement decision-making, the NIS Enforcement Guidelines set out our decision-making arrangements for relevant cases in the DGE sector that Ofgem is responsible for. The decisions will be taken as set out in the relevant paragraphs of the NIS Enforcement Guidelines (see paragraphs 3.38-3.40, 5.10-5.12, 6.10). Ofgem will make relevant enforcement decisions in the DGE sector, having liaised as appropriate with BEIS in the context of our joint CA role. We may also notify other bodies such as the National Cyber Security Centre, where appropriate.

1.36 Regarding introducing formalised special arrangements to assist consistency across sectors or across international borders, we consider some of these matters

are beyond the scope of the NIS Enforcement Guidelines document and would require future negotiation and agreement (potentially involving changes to the NIS Regulations themselves) before such arrangements could be put in place. At present we are not aware of strong evidence to suggest that the existing arrangements are inadequate or that some of the suggested arrangements, such as a lead CA for OES that operate across sectors, may be necessary. Notwithstanding the above, our Guidelines include paragraphs (3.26 – 3.30) clarifying that, as part of our case opening assessment on a case-by-case basis we will have regard, to whether any alleged contravention or failure is also liable to enforcement via another body or under another enactment. This principle would extend to consideration of any action being contemplated by CAs for different sectors or their equivalents overseas where this is known at that stage. The NIS Regulations themselves also set out a requirement to have regard to whether a contravention is also liable to enforcement under another enactment in certain circumstances.[9]

Opening a case

1.37 Many respondents commented on Section 3 of the Guidelines (paragraphs 3.1 – 3.40). In relation to paragraph 3.12, one respondent believed that Ofgem should declare its responsibilities regarding how it will handle sensitive information (alongside asking those who submit information to make Ofgem aware if the information is commercially, security or business sensitive, or whether it relates to an individual's private affairs). Another respondent suggested there should be a "presumption of confidentiality" when handling information rather than placing the onus on those who submit it.

1.38 In relation to paragraph 3.13 one respondent believed OES should be notified in advance of certain information handled by Ofgem being published or disclosed.

1.39 One respondent requested that the word "may" in the first line of paragraph 3.16 should be replaced with "will". The respondent believed OES should always be contacted in advance of case opening (as well as case closing) to clarify and

[9] Regulation 23(2)(e) of the NIS Regulations.

validate information. The respondent expressed concern about the potential reputational damage of publishing details of case openings and closures.

1.40 In relation to paragraph 3.20, one respondent asked that the fifth bullet should include conditional language to allow for circumstances in which providing supporting evidence may not be possible.

1.41 Regarding paragraph 3.24, one respondent asked for further clarification around the meaning of the phrase "priority matter".

1.42 Considering paragraph 3.28, one respondent believed OES should be involved, where possible, in any process of engagement between Ofgem and another enforcement body where that engagement considered how enforcement should proceed.

1.43 In relation to paragraph 3.36, a respondent challenged whether OES co-operation around "self-reporting" should be a relevant factor in determining the likelihood of Ofgem opening an enforcement investigation. The respondent believed that this was not consistent with incident reporting guidance and pointed out that sometimes OES could not devote resource to self-reporting when prioritising live incident management.

1.44 More generally, one respondent requested further provisions to state that OES would be informed appropriately before any enforcement action.

Ofgem response

1.45 We consider our aim of being fair and transparent throughout the enforcement process, as set out in paragraph 1.19, addresses concern about informing OES appropriately before enforcement action.

1.46 In relation to paragraph 3.12, we fully appreciate the potential sensitivities in relation to some information provided to us under or in connection with the NIS Regulations. We will always seek to ensure that information received is handled appropriately depending on the nature of the information in question. Where information disclosure requests are received by public authorities (e.g. under the Freedom of Information regime) these are assessed case-by-case in line with our statutory duties. We therefore cannot apply an automatic 'presumption of confidentiality' as suggested above. We would ask OES to ensure that they clearly mark any information which they consider confidential as such. This will

help us if we need to determine how information should be handled. OES should also seek advice internally before disclosing information where they feel this is appropriate or necessary.

1.47 Regarding paragraph 3.13, we consider that the text reflects certain legal duties that may lead to disclosure of information given to us. We will normally, where appropriate, liaise with an affected OES where onward disclosure is envisaged subject to our statutory duties or any wider factors which may make this inappropriate in a given case.

1.48 For paragraph 3.16, we consider that the "may" qualifier is appropriate. The context concerns the process that occurs in advance of the decision on whether to open a case. In some circumstances we might have collected enough evidence to allow us to make a case opening decision without needing to further involve the OES. In practice it is likely that we will have ongoing engagement with the OES in advance of any case opening decision. When the decision itself to open a case has been taken, we will normally notify the OES as described in paragraph 4.3.

1.49 We note the suggestion of including a qualification in the fifth bullet of paragraph 3.20. However, we consider that the first sentence of that paragraph is clear in stating we will "have regard" to the bulleted statements beneath, including whether they might apply. We do not, therefore, consider that a further qualification is necessary.

1.50 The phrase "priority matter" recognises that Ofgem has limited resources with which to carry out its enforcement activity. Many factors may be taken into consideration when determining priorities, which are set out in paragraphs 3.23-3.36. These paragraphs explain the factors we normally consider when determining whether an issue is a "priority matter" and should be taken forward for enforcement action.

1.51 We note the comment with reference to paragraph 3.28. In practice the OES is likely to be involved in or made aware of discussions that we may be having with other bodies. However, there may be reasons why that might not be the case, so we consider that the current wording is appropriate.

1.52 We note the challenge regarding paragraph 3.36 and how it might relate to other Guidance on voluntary reporting. Considering the challenge, we have opted to remove the previous bracketed statement and make a minor drafting adjustment

to clarify that self-reporting will be taken into account where relevant for our assessment.

Publication of case information

1.53 Some respondents referred to section 8 of the NIS Enforcement Guidelines, which sets out our position on how and when we may make certain case details public.

1.54 One respondent urged caution and that careful management of external communications would be needed; they believed the focus for enforcement cases should be on achieving good outcomes rather than making case information public. Another respondent urged caution given that making information public at the wrong time could have serious adverse impacts on security.

Ofgem response

1.55 We created a dedicated section (section 8) covering our approach to publication of information about enforcement action because we understand the sensitivities, particularly around security. We consider that including a dedicated section is an important step in signalling the seriousness of the matter in the NIS context. Nevertheless, we consider that because "transparency" is a foundational regulatory principle, it is important to position our approach as being "transparent where possible" while recognising that in many cases we may choose not to publish. In addition, where we are considering publishing information, that information may be limited, redacted, delayed, and only published after engagement with the relevant parties as set out in section 8 of the Guidelines. We consider that we have put in place appropriate safeguards and channels of engagement to ensure that we will appropriately consider any relevant concerns before taking decisions to put any NIS enforcement action information in the public domain. However, in light of the feedback, we have made some minor adjustments to the text to further emphasise the importance of security concerns in our decision making.

Other responses

1.56 One respondent referenced the timelines for cases as indicated in paragraph 4.4. The respondent pointed out that changes to timelines and a lack of clear information could cause difficulties for the relevant OES in terms of disruption and

resourcing. The respondent requested that greater emphasis be placed on stronger communication and timely notifications to reduce burdens on OES.

1.57 A respondent commented on the sub-section "Compliance monitoring" in section 7 (paragraphs 7.5 - 7.6). They pointed out that the text stated this "may often be a necessary step" but there was little information to explain how any resultant costs or burdens on OES would be kept to a minimum.

1.58 Regarding section 9 covering appeals, one respondent queried whether the General Regulatory Chamber would have the necessary skills and experience to adequately adjudicate.

Ofgem response

1.59 Regarding appeals we have set out details of the appeals provisions largely as they appear in the NIS Regulations. Any concerns regarding the appeals mechanism should be addressed via the appropriate channels when the NIS Regulations are next reviewed.

1.60 We note the comment about paragraph 4.4 and have made a change to clarify that we may deviate from the provisional timeline where we consider there is good reason to do so and will notify the relevant OES where necessary or appropriate. We have also added a line to paragraph 4.13 to clarify that documents or notices will generally be served electronically (by email) on the current Networks and Information Systems Responsible Officer appointed for an OES.

1.61 On compliance monitoring (paragraphs 7.5 - 7.6), we consider this may often be a necessary outcome of enforcement investigations when we serve an Enforcement Notice. Enforcement Notices will usually set out steps required to rectify contraventions or failures. To verify that required steps, which may have implementation timelines of many months or more, have been adequately taken, we may need to undertake compliance monitoring. We consider that the likelihood of such case outcomes justifies the use of the term "may often be a necessary step". In line with our enforcement vision, we aim to be fair throughout the enforcement process. This extends to any burdens and costs on OES related to post investigation compliance monitoring. In this context we do not consider that additional text is required with reference to this part of the enforcement process.

2. The proposed NIS Penalty Policy

Section summary

This section summarises the consultation responses to the second question in our consultation (shown below) and sets out our responses, including our reasons for deciding to make appropriate changes or retain the original text. The main themes emerging from the consultation responses were a request for a more detailed approach and clarification of terms such as "material contravention".

Question 2: With respect to the NIS Penalty Policy at Annex 1, are the processes for determining penalties clearly presented? We invite respondent's views on any aspect of the proposed penalty policy, including any suggestions for changes or additions.

Stakeholder feedback from the consultation

2.1 Stakeholders were broadly supportive of the new NIS Penalty Policy, which appears as an annex to the main NIS Enforcement Guidelines document. In line with comments on the main NIS Enforcement Guidelines, stakeholders believed the structure was relatively clear and that the proposed process would help provide clarity and transparency around the factors Ofgem would normally consider when determining the amount of a financial penalty under the NIS Regulations.

2.2 However, a broad theme emerged, which can be summarised as a desire for more information to provide greater certainty around the process. There were calls for more detail to help clarify what "material contravention" might mean in practice alongside how the applicable penalty bands would be identified, and assessments of seriousness made.

2.3 Some respondents asked us to consider including examples (e.g. of breach type and consequent penalty levels) to help provide clarity around the differences between the three penalty bands. Another respondent called for the incorporation of a "quantitative methodology" to help improve the Penalty Policy. There was also a call for the creation of a working group and/or workshops to improve understanding and clarity around penalties.

2.4 In terms of detail, one respondent believed more information was required to clarify the meaning of "significant risk" in Regulation 18(6)(d) as a means of helping to determine the difference between the middle and upper penalty bands. Another respondent argued that the definition of a "material contravention" under Regulation 18(7)(a) should not incorporate any failure under Regulation 17(1)(a) unless more clarity could be provided on what "material contravention" might mean in practice. One respondent called for the re-introduction of the fourth penalty band that was present in the original version of the NIS Regulations.

2.5 Another theme to emerge was the connection between NIS penalties and those that might be levied under a different Ofgem regime (e.g. under Ofgem's enforcement powers under the Gas Act 1986 or Electricity Act 1989) or by other enforcers. There was some concern about the possibility of being punished twice for what was effectively the same failure, or a lack of consistency between regimes or enforcers.

2.6 A few other comments regarding the NIS Penalty Policy were received. One respondent pointed out that OES were potentially the victims of a crime, sometimes committed by a highly resourced and capable state actor, when subject to a cyber-attack. That should be taken into consideration, as mitigation, when making any penalty assessment. Another respondent mentioned that some OES might be financially at risk; a penalty could increase that risk so calculations should take that into account. The assessment should also take account of the OES size and financial resources generally. One respondent requested the inclusion of process flowcharts with estimates of the likely timelines for cases.

Ofgem response

2.7 We recognise that this first version of the NIS Penalty Policy, although having several clearly articulated steps, is relatively concise about how, for example, the applicable penalty band will be determined. This approach is by design and reflects that the Policy is new and cannot draw on experience and learnings from previous cases in the DGE sector. Our intention was to not depart too far from the NIS Regulations themselves to mitigate so called "gold plating", or unintentionally creating de facto new rules in guidance. Rather, our intention was to create a reliable, repeatable, and transparent framework within which each case can be considered on its merits. We consider that in future versions of the Penalty Policy we may be able to provide more detail should we be able to draw

generally applicable lessons from the individual cases to which we apply the NIS Penalty Policy.

2.8 Along similar lines, the NIS Penalty Policy positions the term "material contravention" in line with its definition in the NIS Regulations themselves.[10] The Policy merely sets out how determining whether a contravention is a "material contravention" (or not) will itself be a determinant of which of the three penalty bands might apply. We consider that any attempts to go further in scoping out what the term means in practice, or provide real world examples, suffers the risk of unintended consequences such as creating de-facto new rules. We consider there may be opportunities to share case knowledge and examples in an appropriate way, taking care to manage any security or other concerns, as and when the time arises. Currently, we do not have relevant learning from concluded cases from which to draw such material.

2.9 Again, similar logic applies to further clarifying the meaning of "significant risk". We consider this should be determined on a case-by-case basis relying on the available evidence. We are not in favour of trying to provide further information (particularly in the absence of learnings from real NIS enforcement cases) that could have the consequence of "gold-plating" or creating de-facto new rules or policy in guidance or rendering the Policy difficult to apply to future cases.

2.10 In terms of the relationship between NIS enforcement action and a contravention that might be liable to enforcement under another enactment, we consider that the Guidelines are clear (at paragraphs 3.26 – 3.30) that we will take these matters into account as appropriate when making decisions to open or keep open cases. To do that we make clear that we will liaise with other bodies as necessary or appropriate as set out above.

2.11 In relation to the imposition of financial penalties, we will generally have regard to matters such as the need to avoid potentially penalising the same contravention twice where that may be inappropriate. As noted above, Regulation 23 also sets out a number of factors we must have regard to in certain circumstances (including before imposing a penalty). It also requires us to consider whether it is "reasonable and proportionate" to take action in relation to

[10] Regulation 18(7) of the NIS Regulations.

a contravention before we serve a final Penalty Notice. Operators will have an opportunity to provide representations on any proposed penalties and may also raise such points for our consideration at that time.

2.12 The NIS Penalty Policy includes a step (Step 5) that allows for an adjustment to be made to take account of OES financial circumstances where appropriate. As far as the relative size of an OES is concerned, we consider "Step 2" of the Penalty Policy will take account of this, because it considers the impact or potential impact on consumers and other market participants.

2.13 Regarding whether an OES might be a victim of crime, potentially by a state actor, we consider that "Step 2" of the policy can take account of such matters. "Step 2" makes clear that "whether there were adequate internal systems and processes that may have helped prevent the contravention or failure" may be considered; the step may also take into account, where appropriate, "whether the circumstances in which the contravention or failure occurred were within the control of the OES of would have been apparent to an OES acting diligently".

2.14 Finally, we considered the addition of a "process flowchart" but consider that the steps involved in determining penalty amounts are clear enough without this addition.

3. Conclusion and next steps

Conclusion

3.1 Having considered the consultation responses received, the decision of the Authority is to proceed with publishing the first version of the NIS Enforcement Guidelines and Penalty Policy (appended as an Annex to the main Guidelines document).

3.2 The Guidelines will be published with the additions and amendments as set out in this document.