ofgem
Making a positive difference
for energy consumers

Guidance

Network and Information Systems Regulations - Enforcement Guidelines (DRAFT)

Publication date:	[tbc]	**Contact:**	[tbc]
		Team:	Enforcement
		Tel:	020 7901 XXXX
		Email:	NISEGconsultation@ofgem.gov.uk

Overview:

As part of Ofgem's duty to regulate the way in which businesses in the energy sector behave, it is important that we can act swiftly and decisively to put things right if businesses fail to meet their obligations, including where they demonstrate poor behaviours or conduct. By doing so, Ofgem can send strong deterrent messages to all the relevant businesses operating in the energy sector.

This document describes the following:

- how we may use our enforcement powers and tools in situations relating to contraventions of the Network and Information Systems Regulations 2018 ("NIS Regulations");
- how our enforcement decision-making process under the NIS Regulations works;
- how we may serve enforcement and penalty notices on Operators of Essential Services under the NIS Regulations;
- how contraventions will be addressed and deterred; and
- the actions we may take as an alternative to exercising our statutory enforcement powers.

The aim of these guidelines 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 Regulations.

Contents

1. Introduction

1.1. Ofgem is the Office of Gas and Electricity Markets. We are a non-ministerial government department and we work to support the Gas and Electricity Markets Authority.

1.2. Our role is to protect consumers now and in the future by working to deliver a greener, fairer energy system.

We do this by:

- working with Government, industry and consumer groups to deliver a net zero economy at the lowest cost to consumers;
- stamping out sharp and bad practice, ensuring fair treatment for all consumers, especially the vulnerable; and
- enabling competition and innovation, which drives down prices and results in new products and services for consumers.

What does this guidance cover?

1.3. The aim of the Network and Information Systems Regulations 2018[1] (NIS Regulations) is to drive improvement in the protection of the network and information systems that are critical for the delivery of the UK's essential services.

1.4. The NIS Regulations came into force on 10 May 2018[2].

1.5. Designated operators of essential services[3] (OES)[4] must comply with a number of security duties set out in the NIS Regulations.[5] These include taking appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems[6] on which their essential service relies. OES must also take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information

[1] The NIS Regulations implement provisions of the Directive on Security of Network and Information Systems (Directive 2016/1148) which was adopted by the European Parliament on 6 July 2016.
[2] This guidance document reflects the provisions of the NIS Regulations in force as at the date of publication of this guidance and will be interpreted in line with any amendments to the NIS Regulations from time to time. A copy of the NIS Regulations can be found at: https://www.legislation.gov.uk/
[3] An "essential service" means a service which is essential for the maintenance of critical societal or economic activities (see regulation 1(2) of the NIS Regulations).
[4] An "OES" (or "operator of an essential service") means a person who is deemed to be designated by BEIS as an operator of an essential service under regulation 8(1) of the NIS Regulations or is designated as an operator of an essential service under regulation 8(3) of the NIS Regulations (see regulation 1(2) of the NIS Regulations).
[5] See regulation 10 of the NIS Regulations.
[6] Relevant network and information systems are defined in Regulation 1(2) of the NIS Regulations.

systems used for the provision of an essential service, with a view to ensuring the continuity of those services.

1.6. OES also have a duty to notify Ofgem in writing about any incident which has a significant impact on the continuity of the essential service which that OES provides. These are defined as a "NIS incident"[7]. In order to determine the significance of the impact of an incident, an OES must have regard to the number of users affected by the disruption of the essential service, the duration of the incident and the geographical area affected. The notification must contain the information specified in the NIS Regulations and be provided to Ofgem without undue delay and in any event no later than 72 hours after the OES is aware that a NIS incident has occurred[8].

1.7. This guidance provides information on the processes and procedures Ofgem will generally apply when taking enforcement action under the NIS Regulations in relation to OES in the downstream gas and electricity (DGE) sectors.

Status of this guidance

1.8. CAs are required to publish guidance under the NIS Regulations[9] in such form and manner as they consider appropriate. This guidance document applies to enforcement action taken or being considered by Ofgem under the NIS Regulations. We will have regard to this guidance to the extent we consider appropriate.

1.9. We may amend this guidance from time to time and will use the version published on Ofgem's website. If the circumstances of a particular case justify it, we may depart from the general approach to enforcement set out in this guidance.

1.10. Ofgem has also produced a number of other guidance documents to support OES in the DGE sector. These include guidance to support OES in ensuring compliance with the NIS Regulations[10].

1.11. This guidance is not a substitute for any legal provisions and should not be taken as legal advice. OES should consider seeking independent legal or professional advice to ensure they comply with their obligations under the NIS Regulations.

[7] See regulation 11(1) of the NIS Regulations.
[8] Regulation 11(3) of the NIS Regulations. [Details of NIS Incident reporting requirements to be updated].
9 Regulations 3(3)(b) of the NIS Regulations.
[10] [ofgem cyber guidance to be linked once updated]

Ofgem's NIS role

1.12. Ofgem[11] acting jointly with the Secretary of State for Business, Energy and Industrial Strategy[12] (BEIS) is the competent authority (CA) responsible for regulating the activities of OES in the DGE[13] sectors in England, Wales and Scotland[14].

1.13. In the DGE sectors, OES are those operators which are determined by thresholds defined in the NIS Regulations and those determined and designated by BEIS.

1.14. Ofgem is responsible for enforcing compliance with the NIS Regulations in the DGE sectors. This includes investigating potential non-compliance and serving Enforcement Notices and Penalty Notices.

1.15. Certain compliance and enforcement matters in the DGE sectors are normally handled by BEIS (covering OES designation and related issues). Further details of BEIS's enforcement scope can be found in its Policy Guidance for the Implementation of the Network and Information Systems Regulations for the Energy Sector in Great Britain[15].

1.16. BEIS and Ofgem are committed to effective liaison and working arrangements to ensure the maintenance of an effective joint CA for the purposes of fulfilling the requirements of the NIS Regulations.

Vision for our enforcement work

1.17. Our vision for our enforcement work is to achieve a culture where businesses put energy consumers first and act in line with their obligations.

1.18. Our strategic enforcement objectives are to:

- deliver credible deterrence across the range of our functions, stamping out bad and sharp practice and ensuring fair treatment for all consumers, especially those in vulnerable situations;
- enable competition and innovation, which drives down prices and results in better quality and new products and services for consumers, including informal

[11] The Gas and Electricity Markets Authority is the body referred to in the NIS Regulations. Ofgem and the Gas and Electricity Markets Authority are referred to inter-changeably in this guidance.
[12] BEIS is also the CA for the essential services specified in paragraph 2 and paragraphs 3(5) to (8) of Schedule 2 of the NIS Regulations. These cover essential services within the oil subsector and upstream gas sector, including certain gas storage facilities, LNG facilities, gas processing facilities and petroleum production projects. The Health and Safety Executive (HSE) carries out day to day compliance and enforcement functions on behalf of BEIS in these sectors under the terms of an agency agreement.
[13] 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).
[14] Regulation 3(1) and Schedule 1 of the NIS Regulations. The Department of Finance (Northern Ireland) is responsible for these sectors in Northern Ireland.
[15] https://www.gov.uk/government/consultations/implementation-of-the-network-and-information-systems-regulations-in-the-energy-sector-amendments-to-guidance

processes where that will deliver results more effectively;

- ensure visible and meaningful consequences for businesses and, when appropriate, company directors, who fail consumers and who do not comply; and
- achieve the greatest positive impact by prioritising enforcement resources and using the full range of our powers and regulatory "toolkit".

1.19. We aim to achieve these objectives by:

- identifying poor conduct or behaviour early and taking action in a timely manner;
- using a range of appropriate enforcement processes;
- being fair and transparent throughout the enforcement process and, where appropriate, visible in the actions that we take; and
- learning from everything we do, including sharing lessons learned across Ofgem and from across the energy industry.

Regulatory principles

1.20. When undertaking enforcement action, regulation 23 of the NIS Regulations sets out a number of general considerations. Before a CA takes any relevant enforcement action[16] it must consider whether it is reasonable and proportionate on the facts and circumstances of the case to take action in relation to the contravention. We must, in particular, have regard to the following matters:

- any representations made by the OES about the contravention and the reasons for it;
- any steps taken by the OES to comply with the requirements set out in the NIS Regulations;
- any steps taken by the OES to rectify the contravention;
- whether the OES had sufficient time to comply with the requirements set out in the NIS Regulations; and
- whether the contravention is also liable to enforcement under another regulatory regime.

1.21. We will also have regard to the NIS National Strategy[17] when carrying out our duties. The NIS National Strategy sets out strategic objectives and priorities on the security of network and information systems in the UK.

[16] For OES in the DGE sector, this refers to action under: a) regulation 17(1) relating to Enforcement Notices; b) regulation 18(3A) relating to the imposition of financial penalties; or c) regulation A20 relating to enforcement by civil proceedings.
[17] As required by regulation 3(6) of the NIS Regulations. "The National Cyber Security Strategy (2016-

1.22. The Government has also published guidance[18] for CAs to help them carry out their functions under the NIS Regulations. The guidance notes that the process for enforcement action under the NIS Regulations has been designed to give as much flexibility as possible to the CAs as to the process that any enforcement action takes.

1.23. In carrying out our functions under the NIS Regulations, we will consult and co-operate with other relevant authorities[19] where appropriate.

2021): National Cyber Security Strategy 2016-2021 (publishing.service.gov.uk)

[18] "Security of Network and Information Systems - Guidance for Competent Authorities", Department for Digital, Culture, Media and Sport: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701050/NIS_-_Guidance_for_Competent_Authorities.pdf [update before publishing if possible]

[19] As required by regulation 3(3)(g) of the NIS Regulations.

2. Our enforcement powers

2.1. We have a number of powers under the NIS Regulations to support us in our enforcement work. A summary of our key investigative and enforcement powers is set out below.

Power to serve an Information Notice

2.2. We may use information in our enforcement cases that has been obtained from a number of sources (as referred to at paragraph 3.2).

2.3. Before we issue an information notice (Information Notice) using our powers under the NIS Regulations, we may contact an OES to seek clarification or information. Prompt responses may speed up the resolution of the issue and might avoid the need to issue an Information Notice or take other enforcement action.

2.4. Where appropriate, we will use our powers in the NIS Regulations to collect the information and evidence which we need. We can serve an Information Notice[20] in writing upon an OES, requiring it to provide us with all such information as we reasonably require for one or more of the following purposes:

- to assess the security of the OES' network and information systems;
- to establish whether there have been any events that we have reasonable grounds to believe have had, or could have, an adverse effect on the security of network and information systems and the nature and impact of those events;
- to identify any failure of the OES to comply with any duty set out in the NIS Regulations; or
- to assess the implementation of the OES's security policies, including from the results of any inspection conducted under Regulation 16 of the NIS Regulations and any underlying evidence in relation to such an inspection.

2.5. We may need to issue several Information Notices in the course of assessing an issue or concern. We may ask for additional information or clarification after considering material submitted in response to an earlier Information Notice.

2.6. The Information Notice will set out what information is required, the reasons for requesting it, how the requested information should be submitted, and the deadline. We will set the length of any deadline for response based on the complexity of the issues raised and the breadth, type and amount of information required. We will give what we consider, in the circumstances, to be a reasonable amount of time for responses.

[20] Regulation 15(2) of the NIS Regulations.

2.7. In certain circumstances we may share drafts of the Information Notice with the OES to give it an opportunity to comment on the scope or form of the Information Notice (for instance, whether the data or documentation is available in the form requested), and on whether there is any practical issue with the deadline. We will then issue the finalised Information Notice.

2.8. Any problems understanding an Information Notice should be raised promptly. We will aim to deal with all queries promptly and reasonably.

2.9. Delays in the provision of information may have an impact on overall timescales for our decision in an enforcement case. We expect OES to respond within deadlines to the Information Notices served upon them.

2.10. OES must comply with the requirements of an Information Notice. Where an OES fails to comply with an Information Notice, this can lead to service of an Enforcement Notice (see Section 5) and/or a Penalty Notice (see Section 6). Non-compliance may include (among other things) not responding to the Information Notice or any aspect of it, as well as not responding within the specified timescales.

2.11. If we withdraw an Information Notice, we will confirm this in writing to the OES on whom it was served.

Power to inspect

2.12. The NIS Regulations give CAs powers to conduct inspections of OES[21]. An inspection refers to any activity[22] carried out for the purpose of:

- verifying compliance with the requirements of the NIS Regulations; or
- assessing or gathering evidence of potential or alleged failures to comply with the requirements of the NIS Regulations.

This may include any necessary follow-up activity for either of the above purposes.

2.13. Ofgem intends to carry out planned inspections of OES in line with our Inspections Framework[23]. In our enforcement or compliance work with OES, we will use our inspection powers on a case by case basis, where appropriate. Such inspections may need to be carried out at short notice and will follow a different approach to that set out in the Inspections Framework for planned inspections.

2.14. We may conduct all or any part of an inspection ourselves or appoint another party to conduct all or any part of an inspection on our behalf on such terms and in such a

[21] Regulation 16 of the NIS Regulations.
[22] This includes any steps carried out by inspectors in line with their powers set out at regulation 16(5) of the NIS Regulations.
[23] NIS Inspection Framework for Downstream Gas and Electricity dated 5 November 2020.

manner as we consider appropriate. We can also direct an OES to appoint a party who is approved by us to conduct all or any part of an inspection on our behalf.

2.15. Inspections carried out as part of an enforcement process are likely to be tailored to the issues under consideration. We will liaise with an OES at the time to put in place any necessary arrangements.

2.16. An inspector has the power at any reasonable time to enter the premises of an OES (except any premises used wholly or mainly as a private dwelling) if the inspector has reasonable grounds to believe that entry to those premises may be necessary or helpful for the purpose of the inspection[24].

2.17. We will engage with OES to discuss the timing of inspections carried out as part of the enforcement process and provide information about the process, wherever this is appropriate. Where it is appropriate and practicable to do so, we will provide reasonable notice (usually not less than 48 hours) before exercising our power of entry. In exceptional circumstances, we may need to carry out on-the-spot inspections without prior notice or with more limited notice. This might occur, for example, when there has been a NIS incident and we need to assess what further action, if any, is required[25].

2.18. In addition to the power of entry summarised above, an inspector may:

- require an OES to leave undisturbed and not to dispose of, render inaccessible or alter in any way any material, document, information, in whatever form and wherever it is held (including where it is held remotely), or equipment which is, or which the inspector considers to be, relevant for such period as is, or as the inspector considers to be, necessary for the purposes of the inspection;

- require an OES to produce and provide the inspector with access, for the purposes of the inspection, to any such material, document, information or equipment which is, or which the inspector considers to be, relevant to the inspection, either immediately or within such period as the inspector may specify;

- examine, print, copy or remove any document or information, and examine or remove any material or equipment (including for the purposes of printing or copying any document or information) which is, or which the inspector considers to be, relevant for such period as is, or as the inspector considers to be, necessary for the purposes of the inspection;

- take a statement or statements from any person;

[24] Our inspectors will have regard to the Code of Practice on Powers of Entry (Home Office – December 2014) when exercising any functions to which the Code of Practice relates. "Home Office Code of Practice Powers of Entry": Home Office Code of Practice Powers of Entry.
[25] Regulation 11(5)(a) of the NIS Regulations.

- conduct, or direct the OES to conduct, tests;[26]
- take any other action that the inspector considers appropriate and reasonably required for the purposes of the inspection.

2.19. Inspectors will produce proof of their identity if requested by any person present at the premises. Inspectors must also take appropriate and proportionate measures to ensure that any material, document, information or equipment removed is kept secure from unauthorised access, interference and physical damage[27]. Where an inspector removes any document, material or equipment, the inspector will provide, to the extent practicable, a notice giving:

- sufficient particulars of that document, material or equipment for it to be identifiable; and
- details of any procedures in relation to the handling or return of the document, material or equipment.

2.20. Before exercising their powers[28], inspectors are required to take such measures as appear to them appropriate and proportionate to ensure that the ability of the OES, as the case may be, to comply with any duty set out in the NIS Regulations will not be affected. The inspector may consult such persons as appear appropriate to the inspector to ascertain any risks.

2.21. We appreciate the full and prompt co-operation of OES with our inspections. OES are required under the NIS Regulations to:

- pay the reasonable costs of inspection, if so required by us;
- co-operate with inspectors;
- provide reasonable access to their premises in accordance with this power of entry summarised at paragraph **Error! Reference source not found.** above;
- allow the inspector to to examine, print, copy or remove any document or information, and examine or remove any material or equipment, in accordance with the inspector's powers;
- allow the inspector access to any person from whom the inspector seeks relevant information for the purposes of the inspection;

---

[26] A test refers to any process which is: (i) employed to verify assertions about the security of a network or information system; and (ii) based on interacting with that system, including components of that system,
and includes the exercising of any relevant security or resilience management process (see regulation 16)(9)(a) of the NIS Regulations).

[27] This applies where documents, information, material or equipment are removed in accordance with the inspector's powers set out at regulation 16(5)(d).

[28] This applies to the powers of inspectors set out at regulations (5)(b) to (d) and (g) of the NIS Regulations.

- not intentionally obstruct an inspector performing their functions under the NIS Regulations;
- comply with any request made by, or requirement of, an inspector performing their functions under the NIS Regulations.[29]

2.22. In certain circumstances, failure to comply with inspection requirements can lead to service of an Enforcement Notice (see Section 5) and/or a Penalty Notice (see Section 6). This applies where an OES fails to comply with a direction to appoint an approved person to carry out all or any part of an inpection[30] or fails to comply with any of the OES's duties in relation to inspections (summarised at paragraph 2.12 to 2.21 above).

Power to issue an Enforcement Notice

2.23. Where we have reasonable grounds to believe that an OES has failed to comply with certain requirements of the NIS Regulations we may serve an enforcement notice ("Enforcement Notice")[31].

2.24. An Enforcement Notice will be in writing and will specify the reasons for the notice and the alleged failure which is the subject of the notice. We will also set out what steps, if any, must be taken to rectify the alleged failure and the time period during which such steps must be taken.

2.25. An OES upon whom an Enforcement Notice has been served must comply with the requirements, if any, of the notice regardless of whether the OES has paid any penalty imposed on it under regulation 18 of the NIS Regulations.

2.26. Further details about Enforcement Notices, including how they are served and the consequences of non-compliance, are set out at Section 5.

2.27. In certain situations, Enforcement Notices in the DGE sectors may be handled by BEIS (where these relate to OES designation or related issues). Further details can also be found in Section 5.

Power to issue a Penalty Notice

2.28. Ofgem has the power under the NIS Regulations to impose financial penalties in certain circumstances[32].

2.29. We may serve a notice of intention to impose a penalty on an OES if we have reasonable grounds to believe that the OES has failed to comply with a relevant duty under the NIS Regulations and we consider that a penalty is warranted having regard

[29] Regulation 16(3) of the NIS Regulations.
[30] Regulation 16(1)(c) of the NIS Regulations.
[31] Regulation 17(1) of the NIS Regulations.
[32] Regulation 18 of the NIS Regulations

to the facts and circumstances of the case. Further details about Penalty Notices are set out in Section 6.

2.30. The sum of any penalty imposed must be an amount that Ofgem determines is appropriate and proportionate to the failure in respect of which it is imposed and is subject to maximum limits set out in the NIS Regulations.[33] Further details of our approach to determining the level of a penalty can be found in Section 6 and Annex 1.

2.31. In certain situations Penalty Notices in the DGE sectors may be handled by BEIS (mainly where these relate to OES designation or related issues). Further details can also be found in Section 6.

[33] Regulations 18(5) and (6) of the NIS Regulations.

3. Opening a case

3.1. This section describes how we identify and decide whether to open an enforcement case into a potential contravention or failure under the NIS Regulations. We describe the sources of information we most frequently rely on, and how we will handle that information. We explain how we prioritise cases and the factors that are important in helping us determine whether to open an enforcement case. In some situations our concerns may be resolved satisfactorily without opening an enforcement case. We describe here the "Alternative Action" tools that we can use and the criteria that should normally be fulfilled before we determine this form of resolution may be appropriate.

Sources of Information

3.2. The following section describes the sources of information, on which we most frequently rely, in order to assess whether to open a case into a potential contravention or failure. Additionally, this section explains how we handle the information we gather, with a focus on how we treat confidential/sensitive information.

i) Incident Reporting

3.3. Under regulation 11(1) of the NIS Regulations, an OES must notify Ofgem about any NIS incidents. A summary of the notification duties is set out at paragraph 1.6. Appropriate incident reporting will allow us to determine if the OES has complied with its duty to notify NIS incidents, including significant information such as the duration of the incident and its nature and impact.

3.4. Following receipt of an incident report from an OES, we may decide to open an enforcement case, if we believe it is appropriate to do so.

ii) Self-reporting other potential contraventions or failures

3.5. We strongly encourage OES to promptly self-report other potential contraventions or failures that do not constitute a NIS incident as described above. Doing so will allow Ofgem and the OES to determine appropriate steps to rectify the matter quickly and effectively. If contraventions or failures emerge as a consequence of prompt, proactive[34], accurate and comprehensive self-reporting, Ofgem will take that into account, including in our decision on whether or not to take enforcement action. If we decide that enforcement action is required, self-reporting may also be reflected in the level of financial penalty or a decision to pursue Alternative Action to resolve the matter.

[34] Where self-reporting occurs as a result of or coincides with an inspection or other regulatory invervention, it may not qualify as a voluntary submission. Ofgem will take account of the timing, accuracy and extent of any information provided, together with other relevant factors such as any plans for remedial action.

iii) Own initiative enforcement cases

3.6. Our ongoing work with OES may also reveal issues or concerns which need to be further investigated. This could include, for example, reviewing an OES's self-assessment reports, improvement plans and other regular engagement between Ofgem and OES. It might also result from an Ofgem inspection.

3.7. Should any issues or concerns arise following an inspection or other routine engagement with OES, we may decide to open an enforcement case. We may also use information obtained from an inspection or other OES engagement to inform our enforcement work.

iv) Whistle-blowers

3.8. Whistleblowing is when a person or company raises a concern about a wrongdoing, risk or malpractice that they are aware of through their work. It is also sometimes described as making a disclosure in the public interest. We invite contact from parties who may have such information relating to the DGE sector. Disclosures made to "blow the whistle" about concerns regarding potential breaches of relevant regulations or legislation may lead to enforcement and/or compliance action.

3.9. To facilitate such disclosures, government has issued whistleblowing guidance[35] applicable to people considering disclosing information, which:

- sets out the circumstances in which disclosure would entitle a person to benefit from the legal protections (against victimisation or unfair dismissal by their employer) offered to whistle-blowers; and
- details the process that should be followed in dealing with whistle-blowers.

3.10. We have also produced our own whistleblowing guidance document[36], which should be consulted before making a disclosure to us.

v) Other sources of information

3.11. Ofgem is able to collect information from a range of different sources, including other CAs. While some information may be gathered via our own inspections and other information gathering powers we might open an investigation following a complaint received by an industry participant, or after receiving information from another CA or other source.

[35] https://www.gov.uk/whistleblowing. The documents include a list of prescribed people and bodies to whom you can blow the whistle. Ofgem is the Gas and Electricity Markets Authority for these purposes.
[36] https://www.ofgem.gov.uk/ofgem-publications/83570/whistleblowingguidance.pdf.

Handling Information

3.12. Following the receipt of information regarding a potential contravention or failure under the NIS Regulations, we may decide to open an enforcement case. Those who submit information to us should make us aware whether the information is commercially, security or business sensitive, or whether it relates to an individual's private affairs. If disclosure of the information might significantly harm a business or a person, a separate non-confidential version of the information should also be submitted to us.

3.13. NIS-related issues are sensitive and Ofgem is mindful of the harm that disclosure might cause, though information provided to us, including personal information, may be published or disclosed in accordance with the access to information regimes (primarily the Data Protection Act 2018, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004) or to facilitate the exercise of our functions.

3.14. We may also share information with other parties in certain circumstances as set out in the NIS Regulations[37]. This includes sharing information with other CAs, relevant law-enforcement authorities and the Computer Security Incident Response Team (CSIRT)[38] where that information sharing necessary for:

- the purposes of the NIS Regulations or of facilitating the performance of any functions of a NIS enforcement authority under or by virtue of the NIS Regulations or any other enactment;
- national security purposes; or
- purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution.

3.15. The NIS Regulations set out a number of safeguards in relation to information-sharing. These include that any information-sharing under Regulation 6 must be limited to information which is relevant and proportionate. There are also provisions requiring the recipient authority not to further share such information for any purpose other than a purpose mentioned above unless otherwise agreed with the relevant NIS enforcement authority.

Initial inquiry phase

3.16. Before a decision is taken to open a case, we may seek further information or clarification from the relevant OES. Prompt responses may speed up resolution of the issue under consideration and increase the likelihood that enforcement action won't be

[37] Regulation 6 of the NIS Regulations.
[38] GCHQ (the Government Communications Headquarters) is designated as the CSIRT for the United Kingdom under regulation 5 of the NIS Regulations. The National Cyber Security Centre, within GCHQ, provides leadership on cybersecurity issues.

taken. We may also seek information from third parties such as our joint CA (BEIS), other CAs or other government partners, to help our assessment.

Alternative Action

3.17. In certain circumstances, Alternative Action may be used to bring an OES into compliance and remedy the consequences of any contravention or failure. Alternative Action can be used in lieu of opening an investigation into a potential contravention or failure, as part of closing a formal investigation or during an investigation to address ongoing concerns.

3.18. In many circumstances Alternative Action will not be appropriate when addressing potential breaches of the NIS Regulations. However, there may be circumstances in which Alternative Action could lead to an effective resolution. When determining whether Alternative Action may be suitable for effectively resolving an issue we will have regard to our prioritisation criteria for opening an investigation (see paragraphs 3.23 – 3.36 below).

3.19. We may pursue one or more of the following Alternative Actions with the OES in question:

- agree a period and a specified format of reporting, either to ensure that behaviour is not repeated or to demonstrate that the OES has taken certain action to adequately address the issue;
- arrange an inspection under Regulation 16 of the NIS Regulations focussed on the particular area (or areas) of concern with the OES agreeing to implement recommendations as necessary;
- arrange for the OES to engage independent auditors or other appropriately skilled persons to conduct a review on the particular area (or areas) of concern with the OES agreeing to implement recommendations as necessary;
- accept agreed voluntary undertakings or assurances to ensure future compliance; or
- the OES agreeing to other voluntary action, such as implementing specified remedial or improvement actions and/or making voluntary payments to:

  i) parties that may have suffered harm as a result of the potential contravention or failure; and/or
  ii) Ofgem's voluntary redress fund to reflect the seriousness of the potential contravention or failure.

3.20. If we decide that Alternative Action is suitable for resolving an issue, we will need to be satisfied that the action will fully address our concerns. In making this decision we will have regard to whether:

- where issues have been self-reported (and are not NIS incidents as defined in regulation 11 of the NIS Regulations), we are satisfied the full extent of the potential contravention or failure has been self-reported promptly, accurately and comprehensively by the OES;

- where issues have come to light via other means, we are satisfied that the full extent of the potential contravention or failure has been established;
- where applicable, we are satisfied that the OES has fully complied with the duty to notify NIS incidents (see paragraph 1.6);
- we are confident that the OES will act promptly to remedy the matter, including taking account of its willingness, ability and its previous compliance record;
- the OES has provided robust assurances (including supporting evidence where necessary) that the potential contravention or failure will not recur; and
- the issue can be adequately addressed by the Alternative Action and be implemented effectively.

3.21. We expect OES to engage fully and proactively in helping to ensure a successful resolution of Alternative Action. If we are not satisfied with an OES's response during Alternative Action we may revert to opening an enforcement case or expanding the scope of an existing enforcement case. Either course of action may include issuing an Enforcement Notice and/or Penalty Notice. Similarly, we will take seriously any evidence that an OES has reneged on assurances, voluntary undertakings or other agreements that form part of an Alternative Action resolution.

3.22. When Alternative Action has led successfully to a satisfactory resolution to an issue we will generally close the matter. If Alternative Action has been used to resolve an issue or issues in an already open enforcement case, we may close it. One outcome of an Alternative Action resolution, however, could be a period of compliance monitoring after closure.

Prioritisation criteria for deciding whether to open (or keep open) an Enforcement case

3.23. In this section we set out the factors we will normally take into account when deciding whether or not to open (or keep open) an enforcement case. These details are non-exhaustive; each issue for which potential enforcement action is being discussed will be considered on its merits taking account of relevant evidence, legal context and resource considerations.

3.24. When making our assessment we will consider the following three criteria:

(1) Do we have the power to act and are we best placed to act?

(2) Is it a priority matter for us due to the apparent seriousness of the potential contravention or failure?

(3) Is it a priority matter for us due to the apparent poor conduct of the relevant OES?

3.25. Provided that criterion (1) is fulfilled we may decide to open a case if only one of the other criteria apply (both need not apply).

Do we have the power to take enforcement action and are we best placed to act?

3.26. This means considering whether the alleged contravention or failure falls within the scope of the NIS Regulations and is a matter for which Ofgem could take enforcement action.

3.27. We will have regard to whether the alleged contravention or failure is also liable to enforcement by another body or under another enactment. This might include, for example, action by the Information Commissioner's Office[39], BEIS or HSE.

3.28. If we identify that an alleged contravention or failure is also liable to enforcement by another body, we will normally discuss the best approach with that body before reaching a decision on how to proceed.

3.29. In certain circumstances we may still take action when another body is already investigating or taking action. Whether an additional investigation may be justified will depend on the circumstances of the case. We will take into account the impact of any action already taken, or to be taken by another body, before deciding whether to open a case into any alleged contravention or failure.

3.30. We are more likely to open a separate enforcement case if, for example:

- the action being taken by the other body appears not to deal with our concerns fully or does not cover all of the matters about which we have concerns;
- a financial penalty may be merited (which the other body does not have the power to impose); or
- separate action should be taken as a deterrent to the relevant OES or others.

Is it a priority matter for us due to the apparent seriousness of the contravention or failure?

3.31. This means assessing a range of factors including the degree to which the suspected contravention or failure is causing or is likely to cause harm (directly or indirectly) to consumers or members of the public. We will also assess whether the suspected contravention or failure is causing or is likely to cause harm (directly or indirectly) to other market participants. We will assess both financial and non-financial aspects of harm and consider whether the OES may have benefited financially or otherwise.

3.32. We will also take account of the extent to which the suspected contravention or failure could harm our ability to regulate effectively and the need to deter poor practice by the OES in question or by others across the market.

[39] For example, under the Data Protection Act 2018.

Is it a priority matter for us due to the apparent poor conduct of the OES in question?

3.33. This means assessing a range of factors including whether the OES is willing and able to comply with its obligations or whether it has recurring poor behaviours or conduct. This assessment may include where apparent poor conduct has given rise to a suspected contravention that is not material.[40]

3.34. Our assessment will include whether the alleged breach appears to be intentional, a sign of negligence or constitutes a failure to comply with previous undertakings.

3.35. In considering the OES's record, we will include any history of similar breaches, including any that in isolation may not have been considered serious enough at the time to justify opening a new case.

3.36. Also, we will consider whether the OES self-reported promptly, accurately and comprehensively (excluding the NIS requirement to report NIS incidents), and whether it is taking timely action (or has already acted) to put matters right. We are more likely to open an investigation if the alleged contravention or failure is ongoing, but can take action if the company is no longer in breach. We are more likely to open an investigation where the OES has not co-operated fully with our enquiries in relation to the potential contravention or failure (including co-operation with any inspection under regulation 16(1)).

Other case opening considerations

3.37. The case opening criteria set out above are not exhaustive; we may consider other factors where relevant such as the risks around opening a case and the resources we have available at the time. On occasion, particularly when addressing a concern across the market, we may not open a case at that stage and instead focus our resources on a relevant compliance exercise which may better address the identified non-compliant conduct and any resulting harm.

Case opening decision-making

3.38. NIS case opening decisions will normally be made by a senior civil servant with responsibility for enforcement matters. In many cases, this will follow a discussion by Ofgem's Enforcement Oversight Board (EOB).

3.39. The EOB provides strategic oversight and governance for all our enforcement work and oversees the portfolio of cases. For NIS case opening decisions, we will generally take into account the prioritisation criteria set out in this section along with any other case opening considerations. Decisions on whether to accept Alternative Action as an

[40] Material contraventions (and by inference contraventions that are not "material") are defined in Regulation 18(7)(a).

acceptable means of resolving an issue or concern (see paragraph 3.17 – 3.22 above) will also normally be taken following an EOB discussion.

3.40. The members of the EOB are usually senior civil servants from across Ofgem. It is chaired by a senior civil servant with responsibility for enforcement.

4. Conducting investigations

4.1. This section sets out the general procedures we will follow once we have decided to open an enforcement case. It explains how we will notify the relevant OES, maintain contact and gather information.

4.2. In certain situations enforcement cases in the DGE sector may be handled by our joint CA (BEIS). This may occur where issues relating to OES designations or related matters are at issue. The relevant OES will be informed by Ofgem or BEIS, as the case may be, about the handling of any enforcement case.

Notification that we are opening a case

4.3. When we open a case we will normally inform the OES under investigation. We may not, for example, where we consider that alerting the OES may prejudice or hamper the investigation. In these cases, we will notify the OES if and when it is appropriate to do so.

4.4. When notifying the OES, we will provide an outline of the alleged contravention or failure and the scope of the enforcement case. We will give a provisional timeline for the key steps and when we expect to give updates. The timeline may change as the case progresses; if it does we will normally notify the OES.

4.5. The scope of the case may widen if we become aware of other matters requiring investigation. The OES may wish to comment on the alleged contravention or failure at this stage (for example, to say that it admits or denies contraventions or failures).

Contact with the case team and meetings

4.6. When we open an enforcement case we will normally provide the OES with contact details of an Ofgem person who will be the main point of contact for the investigation. If an OES has any issues or concerns during the case, they can contact the main point of contact for assistance.

4.7. Meetings between Ofgem and the OES may be held as part of an information or evidence-gathering exercise, or be used to provide updates on the progress of the investigation.

4.8. If we think a meeting is necessary or would be helpful, we will contact the OES with our request. We may request that particular people attend from the OES, such as those with knowledge of the relevant issues under consideration and/or who have the authority to speak for the OES.

Information Gathering

4.9. We may use our powers under the NIS Regulations to collect the information and evidence we need to carry out our investigatory work. During an investigation we may therefore issue one or more Information Notices to obtain the evidence we need. The circumstances in which we may issue an Information Notice are set out in Section 2, paragraphs 2.2 – 2.11 above). Please also refer to those paragraphs for further

information about Information Notices and the things we take into account when identifying deadlines for responses.

4.10. In some circumstances we may also use our powers to conduct inspections to gather information necessary to effectively carry out an investigation. The NIS Regulations include powers for CAs to conduct an inspection (or appoint another party to conduct an inspection on our behalf or direct an OES to appoint a party who is approved by us to conduct an inspection). Further information about our powers to inspect is set out in Section 2, paragraphs 2.12 - 2.22 of this document.

4.11. We may use or seek information and evidence from third parties such as whistle-blowers, other witnesses, other stakeholders or from publicly available records. We may also make use of evidence already collected by Ofgem, such as that collected via a routine inspection.

Investigations timescales

4.12. We aim to carry out investigations as quickly as possible. A provisional timeline will normally be shared with the OES at the outset of a new enforcement investigation; it will be set on a case-by-case basis. The timeline may be updated as the case progresses.

Service of documents and notices

4.13. Where any document or notice is required or authorised to be served on an OES under the NIS Regulations, we will normally serve electronically (by email) in accordance with Regulation 24 of the NIS Regulations.

5. Serving Enforcement Notices

5.1. This section describes how and when we may serve an Enforcement Notice[41]. We describe the circumstances in which we may issue an Enforcement Notice and provide information about how decisions to issue Enforcement Notices are made.

5.2. An Enforcement Notice may be used at different stages during an investigation. In some circumstances an Enforcement Notice might be served at a late stage during an investigation. In other circumstances (e.g. where we already have the evidence we need), we may decide to serve an Enforcement Notice when we open a new investigation or during the course of an investigation.

5.3. An Enforcement Notice may be served before any associated Penalty Notice, alongside an associated Penalty Notice or, occasionally, after an associated Penalty Notice has been served.

Service of an Enforcement Notice

5.4. Ofgem may serve an Enforcement Notice upon an OES if we have reasonable grounds to believe that the OES has failed to:

- notify the CA as required under regulation 8(2) that it falls within the provisions for "deemed" designation as an OES;[42]
- comply with the requirements stipulated in regulation 8A relating to the nomination by an OES of a person to act on its behalf in the United Kingdom;
- fulfil the security duties of OES under regulations 10(1) and (2) (see summary at paragraph 1.5);
- notify a NIS incident under regulation 11(1) (see summary at paragraph 1.6);
- comply with the notification requirements stipulated in regulation 11(3) relating to NIS incidents (see summary at paragraph 1.6);
- notify an incident as required by regulation 12(9);
- comply with an Information Notice issued under regulation 15 (see summary at paragraphs 2.2 – 2.11); or
- comply with:
    - a direction given under regulation 16(1)(c) to appoint an approved person to conduct an inspection (see paragraph **Error! Reference source not found.**); or

[41] Regulation 17 of the NIS Regulations.
[42] "Security of Network and Information Systems Regulation" https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721357/FINAL_NIS_Policy_Document_to_the_Energy_Sector_.pdf

- the requirements for inspections stipulated in regulation 16(3) (see summary at paragraph **Error! Reference source not found.**).

5.5. We will take account of regulation 23 of the NIS Regulations before serving an Enforcement Notice (see paragraph 1.20).

5.6. Before serving an Enforcement Notice we will inform the OES, in such form and manner as we consider appropriate having regard to the facts and circumstances of the case, of the alleged failure and how and when representations in relation to it (and related matters) can be made. We will give the OES a reasonable opportunity to respond taking into account factors such as the complexity of the alleged failure. In certain circumstances (for instance where we need to urgently address ongoing harm) an OES may be expected to respond within a short period of time.

5.7. When we inform the OES as set out above, we may also provide notice of our intention to serve an Enforcement Notice. We may share a draft Enforcement Notice with the OES at this time, although this may not be possible in all cases (e.g. in cases where we need to act quickly to address ongoing harm).

5.8. We may serve an Enforcement Notice on an OES within a reasonable time, irrespective of whether we have provided notice of our intention to serve an Enforcement Notice, having regard to the facts and circumstances of the case, after we have informed the OES about the alleged failure in accordance with paragraph 5.6.

5.9. We will have regard to any representations made by the OES in accordance with paragraph 5.6 above. If an OES wishes us to consider any additional evidence, this should be submited alongside its representations and within any time period stipulated.

Enforcement Notice Decisions

5.10. Decisions on whether (or not) to issue an Enforcement Notice will normally be made by a senior civil servant. This will often follow a meeting of the EOB, where appropriate and timing permits. The EOB acts in an advisory capacity on Ofgem's enforcement activities (see paragraphs **Error! Reference source not found.** – **Error! Reference source not found.**).

5.11. Certain matters may be referred to our Enforcement Decision Panel ("EDP") for a decision. The EDP consists of a pool of members who are employees of the Gas and Electricity Markets Authority, one of whom is appointed as the EDP Chair. EDP members are employed specifically for EDP duties and work independently from the case team.

5.12. The EDP Terms of Reference are published on the Ofgem website[43]. The identity of the panel members will generally be notified to the OES in writing by the EDP Secretariat.

[43] "Committes of the Authority – Terms of Reference "
https://www.ofgem.gov.uk/system/files/docs/2021/02/committee_tors_amended_09022021.pdf

The EDP Secretariat provides administrative and procedural support to the EDP members. The Panel, or its individual members, should not be contacted directly by any party or their representatives.

Action following service of Enforcement Notices

5.13. An OES upon whom an Enforcement Notice has been served must comply with the requirements, if any, of the notice regardless of whether it has paid any penalty imposed on it under regulation 18 (see Section 6).

5.14. We may commence civil proceedings against an OES where we have reasonable grounds to believe that it has failed to comply with the requirements of an Enforcement Notice[44]. We may commence civil proceedings regardless of whether the relevant OES has paid any penalty imposed on it in relation to the contraventions or failure(s) described in the Enforcement Notice.

5.15. Failure to comply with the requirements of an Enforcement Notice may also lead to service of a Penalty Notice (see Section 6).

5.16. An OES may appeal the decision to serve an Enforcement Notice (see Section 9).

OES right to request reasons for an Enforcement Notice decision to take no further action

5.17. If we are satisfied that no further action is required, having considered any representations submitted in accordance with paragraph 5.6 or any steps taken to rectify the alleged failure, we will inform the OES in writing as soon as reasonably practicable.

5.18. Should the relevant OES wish to be provided with reasons why a decision to take no further action in relation to an Enforcement Notice was taken, they can request these within 28 days of being informed of the decision. Upon receiving such a request we will provide our reasons in writing within a reasonable time and no later than 28 days after receipt.

[44] Regulation 20A of the NIS Regulations.

6. Serving Penalty Notices

6.1. This section describes the circumstances in which we may serve a notice of intention to issue a penalty and potentially follow up with a confirmed Penalty Notice[45]. It describes how we make penalty decisions and how OES can respond. We also explain how we can enforce penalties and where the proceeds of penalties go.

6.2. We cover briefly how the amount of a penalty is determined, but please refer to our penalty policy (Annex 1) for fuller details.

Circumstances in which a Penalty Notice may be served

6.3. We will take account of regulation 23 of the NIS Regulations before serving a Penalty Notice (see paragraph 1.20).

6.4. We may serve a notice of intention to impose a penalty upon an OES if the OES has failed to comply with certain duties the NIS Regulations and we consider that a penalty is warranted having regard to the facts and circumstances of the case. The relevant duties are:

- those duties set out in regulation 17(1) of the NIS Regulations (see summary at paragraph **Error! Reference source not found.**); or
- the duty set out in regulation 17(3A) to comply with the requirements of an Enforcement Notice.

6.5. A notice of intention to impose a penalty will be provided in writing to the relevant OES and will specify:

- the reasons for imposing a penalty;
- the sum of the penalty we intend to impose and how the penalty is to be paid;
- the date on which the notice of intention to impose a penalty is given;
- the period within which the penalty must be paid if a Penalty Notice is subsequently served;
- that the payment of a penalty under a Penalty Notice (if any) is without prejudice to the requirements of any Enforcement Notice (if any); and
- how and when the OES may make representations about the content of the notice of intention to impose a penalty and any related matters

[45] Regulation 18 of the NIS Regulations.

6.6. After considering any OES representations we may serve a Penalty Notice with a final penalty decision if we are satisfied that a penalty is warranted having given regard to the facts and circumstances of the case.

6.7. A Penalty Notice will be provided to the OES in writing and will include reasons for the final penalty decision. The Penalty Notice will require the OES to pay either the penalty amount specified in the notice of intention, or an adjusted penalty determined to be appropriate in light of any representations made by the OES or any steps taken by the OES to rectify the failure (including one or more steps required by an associated Enforcement Notice). The Penalty Notice will also specify the period within which the penalty must be paid ("the payment period") and the date on which the payment period is to commence.

6.8. The Penalty Notice is also required to provide details of the appeal process under regulation 19A (see Section 9) and specify the consequences of failing to make payment within the payment period.

How the penalty amount will be determined

6.9. The sum that we impose under a Penalty Notice must be an amount that we determine is appropriate and proportionate to the relevant failure or failures under consideration. The amount that can be imposed is also subject to the maximum amounts detailed in the NIS Regulations[46]. Please refer to our penalty policy (Annex 1) for further information about how we will determine the amount of any penalty.

Decision-making on penalties

6.10. NIS penalty decisions may be made by a senior civil servant. This will generally following a meeting of the EOB which acts in an advisory capacity on Ofgem's enforcement activities. Certain cases may be referred to the the EDP for a decision. Further details about the EDP are set out at paragraph 5.11.

Withdrawal of a Penalty Notice

6.11. If we withdraw a Penalty Notice, we will inform the OES upon which it was served in writing.

Enforcement of Penalty Notices

6.12. Ofgem may take action to enforce or recover penalties if they are not paid[47].

[46] Regulation 18(6) of the NIS Regulations.
[47] Regulation 20 of the NIS Regulations. In England and Wales, a penalty is recoverable as if it were payable under an order of the county court or of the High Court. In Scotland, a penalty may be enforced

6.13. We will not take action to recover a penalty if an appeal has been brought by the relevant OES (see Section 9) and that appeal has not been determined or withdrawn[48].

in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom

[48] Regulation 20(6) of the NIS Regulations.

7. Closing cases

7.1. An enforcement case may be closed at any point. For example, a case may not be pursued if we decide that the issue no longer meets the criteria identified for opening a case (see Section 3 paragraphs 3.23 – 3.36).

7.2. Other situations in which we might close an enforcement case include where:

- we are satisfied that no contravention or failure of the NIS regulations has taken place;
- the contravention or failure has been rectified via Alternative Action resolution;
- an OES has taken adequate steps to rectify the contravention or failure following the issue of an Enforcement Notice; or
- an OES has taken adequate steps to rectify the contravention or failure following the issue of a Penalty Notice.

7.3. There may be other circumstances in which we will close cases. These include decisions taken by Ofgem that the case needs to be closed on the grounds of administrative priorities.

7.4. We will notify OES of case closures in writing as soon as reasonably practicable.

Compliance monitoring

7.5. Upon closure of an enforcement case, Ofgem may wish to engage in a compliance monitoring phase of the relevant OES. This may happen when, for example, we need to monitor whether the OES remains compliant or delivers compliance according to an agreed timeline.

7.6. We consider that extended compliance monitoring may often be a necessary step, because rectification of contraventions or failures may occur over the course of a significant period of time

Feedback

7.7. Ofgem may wish to obtain feedback from the OES upon closing an investigation in order to evaluate the case process and to identify possible improvements for future enforcement cases.

8. Approach to publishing information about enforcement action

8.1. In achieving our enforcement objectives (see paragraphs 1.17 – 1.19) we aim to be transparent and visible in the actions that we take.

8.2. While aiming to be as transparent as possible, we also place importance on concerns around confidentiality, any potential impact on our ability to investigate and other concerns such as security. Security is likely to be a particularly relevant factor for NIS enforcement work given the issues involved. We will have regard to national security matters and other relevant considerations when reaching decisions about making case details public.

8.3. We always seek to ensure parties under investigation are treated fairly and appropriately; we are accountable for the decisions we take and relevant information we make public. This sections provides details of the issues we will consider when making cases public.

NIS incidents

8.4. The NIS Regulations require OES to notify their CA about any NIS incidents (see paragraph 1.6).

8.5. After we have received notification of a NIS incident we may inform the public about it, as soon as reasonably practicable, if we are of the view that public awareness is necessary in order to handle that incident or prevent a future incident[49].

8.6. We may take this course of action whether or not a NIS incident is the subject of an enforcement case, or becomes the subject of an enforcement case.

8.7. A decision on whether to inform the public after receipt of notification of a NIS incident can also be taken by the CSIRT.

8.8. Before Ofgem or the CSIRT informs the public about a NIS incident, we will consult with one another. We will also consult with BEIS, our joint CA, and the relevant OES will also be consulted.

Enforcement case openings

8.9. Our general approach for enforcement case openings outside the NIS Regulations is to publish on our website, unless this would adversely affect the investigation (for example, where it may prejudice our ability to collect information), harm the public

[49] Regulation 11(7)(b) of the NIS Regulations.

interest or is subject to security, confidentiality or other concerns that would make publishing details (or some details) inappropriate.

8.10. In practice, for cases under the NIS Regulations, given sensitivities and concerns around security, we may choose not to publish any case opening information in certain cases, or, as an alternative, we may redact information or publish limited information as appropriate.

8.11. We will consider what information, if any, to make public on a case-by-case basis.

8.12. When we do publish the opening of a case on our website, we will make clear that this does not suggest we have already reached finding(s) about non-compliance.

8.13. In some cases, we may decide to make an announcement to the media. We will normally inform an OES before we publish the opening of a case on our website or make an announcement to the media. We may also seek advice from BEIS, our joint CA, and/or the NCSC before making case openings public.

Enforcement case closures

8.14. Our general approach is to publish case closures on our website. For some cases we may decide to make an announcement in the media. The details of decisions made and communicated to OES in Enforcement Notices or Penalty Notices may be placed in the public domain unless there are compelling reasons not to.

8.15. In practice, given sensitivities and concerns around security, we may choose not to publish case closure information in certain cases, or, as an alternative, we may redact information or publish limited information as appropriate on a case-by-case basis after discussion with our joint CA (BEIS) and/or the NCSC.

8.16. We will consider what information about cases closures, to make public on a case-by-case basis.

8.17. We will normally inform an OES before we publish the closing of a case on our website or make an announcement to the media.

8.18. In order to ensure the transparency of our work, to explain our expectations or to share lessons learned, details of cases resolved via Alternative Action may be made public subject to an assessment of similar factors (particularly around potential security concerns) that apply for case openings and closures.

8.19. When a case has been made public on opening, then if we close it with no finding of breach or infringement (for example, due to lack of evidence, on the grounds of administrative priorities or because we are taking Alternative Action) we may also make this fact public.

8.20. We may also seek feedback following case closure and share lessons learnt in accordance with these guidelines.

9. Appeals

9.1. OES have the right to appeal against certain decisions under the NIS Regulations. This includes the decision to serve Enforcement Notices and Penalty Notices.

9.2. Appeals should be made to the First-tier Tribunal (General Regulatory Chamber) (the "Tribunal") in accordance with the provisions of the NIS Regulations[50] and the Tribunal's applicable rules. The Tribunal is responsible for handling appeals against decisions made by regulatory bodies in a number of areas. The Tribunal is independent of Ofgem and will listen to both sides of the argument before it reaches a decision.

9.3. OES should ensure that they consult the Tribunal's rules to ensure that any appeals are made on time, as well as ensuring that any appropriate legal advice is obtained[51].

9.4. The Tribunal will determine the appeal after considering the grounds of appeal and by applying the same principles as would be applied by a court on an application for judicial review.

9.5. The Tribunal may, until it has determined the appeal and unless the appeal is withdrawn, suspend the effect of the whole or part of the decision to which the appeal relates. OES should refer to the Tribunal rules and seek appropriate legal advice if they wish to apply to the Tribunal for a stay (or, in Scotland, sist) or suspension of an Enforcement Notice or Penalty Notice decision which is or may be the subject of an appeal to the Tribunal pending such appeal[52].

9.6. When it has considered the issues the Tribunal may:

- confirm any decision to which the appeal relates; or
- quash the whole or part of any decision to which the appeal relates.

9.7. Where the Tribunal quashes the whole or part of a decision, it will refer the matter back to us with a direction to reconsider and make a new decision having regard to the Tribunal ruling.

---

[50] Further information about the appeals process, including the admissible grounds of appeal, are contained in Regulation 19A and 19B of the NIS Regulations.
[51] An appellant OES must start proceedings before the Tribunal by sending or delivering to the Tribunal a notice of appeal so that it is received in accordance with the Tribunal's rules. This is generally required within 28 days of the date on which notice of the act or decision to which the proceedings relate was sent to the appellant. The Tribunal's rules may be amended from time to time and OES must ensure that they consult the Tribunal rules directly or seek appropriate legal advice to ensure that an appeal is made on time and in compliance with the relevant requirements. The Tribunal's rules can be found on its website: www.gov.uk/courts-tribunals/first-tier-tribunal-general-regulatory-chamber
[52] Further information about the appeals process, including the admissible grounds of appeal, are contained in Regulation 19A and 19B of the NIS Regulations.

9.8. The new decision, having been made regarding the direction of the Tribunal, will be considered final.

Annex 1 – NIS Penalty Policy

Our primary objective in issuing a Penalty Notice under the NIS Regulations is to promote high behavioural standards amongst OES. We aim to address the contravention or failure and deter OES from committing similar contraventions or failures in the future.

This Annex sets out the factors we will normally consider when determining the amount of a financial penalty under the NIS Regulations.

In the event of an enforcement case concluding that there have been multiple contraventions or failures, we may apply the steps set out in this policy to each of the contraventions or failures in turn where this would be appropriate in accordance with the NIS Regulations.

Determining whether a Penalty Notice should be served

Information on the circumstances in which a Penalty Notice can be served under the NIS Regulations can be found at Section 6 of this guidance.

Framework for determining the penalty amount

The sum of any penalty imposed must be an amount that the Authority determines is appropriate and proportionate to the failure in respect of which it is imposed and in accordance with the penalty categories amounts set out under Step 1 below[53].

If we have decided that it is appropriate to serve a Penalty Notice in a case, we will then follow the four steps set out below, in respect of each contravention or failure, to determine the appropriate overall penalty amount.

Step 1 – Assess the contravention or failure and identify the applicable penalty category

The NIS Regulations identify three capped penalty categories. The first step in calculating the amount of any penalty is therefore to identify the category which best reflects the nature of the contravention or failure. While the NIS Regulations identify categories with an upper cap, no minimum amounts are identified. In identifying the correct penalty category for any contravention or failure, we will apply the following criteria in accordance with the NIS Regulations[54]:

- a category one penalty will be identified for any contravention or failure which we determine was not a Material Contravention. A category one penalty will not exceed £1,000,000;
- a category two penalty will be identified for any Material Contravention which we determine does not meet the criteria set out for a category three penalty. A category two penalty will not exceed £8,500,000;

[53] Regulation 18(5) of the NIS Regulations.
[54] Regulation 18(6) of the NIS Regulations.

- a category three penalty will be identified for any Material Contravention which we determine has or could have created a significant risk to, or significant impact on, or in relation to, the service provision by the OES. A category three penalty will not exceed £17,000,000.

In practice this step will firstly involve determining whether the contravention or failure was a Material Contravention. Any contravention or failure which is not a Material Contravention will fall into category one as set out above. Please see the note below on the meaning of "Material Contravention".

Where a contravention or failure is a Material Contravention, we will determine whether a category two or category three penalty will apply. The key determinant is whether the contravention or failure "has or could have created a significant risk to, or significant impact on, or in relation to, the service provision by the OES". This will be determined on a case-by-case basis in response to our assessment of the evidence.

Step 2 – Assess the contravention or failure and place within the identified penalty category

We will next identify an amount which reflects the contravention or failure within the relevant penalty category. The factors listed below generally consider the nature and impacts of the contravention or failure and the behaviour of the OES in relation to how it occurred. Factors we will consider may include but are not limited to:

- the degree to which energy consumers or members of the public suffered, or could have suffered, harm (financially or otherwise) resulting from the contravention or failure;
- the degree to which other market participants suffered, or could have suffered harm (financially or otherwise) resulting from the contravention or failure;
- the degree to which the OES benefited (financially or otherwise) from the contravention or failure;
- the duration of the contravention or failure;
- whether the contravention or failure was deliberate;
- the degree to which senior management or other responsible individuals were involved in or knew about the contravention or failure and failed to take steps to prevent, mitigate or report it;
- whether there were adequate internal systems and processes that may have helped prevent the contravention or failure; and
- whether the circumstances in which the contravention or failure occurred were within the control of the OES or would have been apparent to an OES acting diligently.

Step 3 – Consider aggravating and mitigating factors

Having established the penalty category and the appropriate penalty level within the category, we will next consider an adjustment to reflect any relevant aggravating or mitigating factors. These factors generally relate to matters including (without limitation):

i) the OES' compliance history; and

ii) the OES' actions (or lack thereof) after it becomes aware of the contravention or failure, whether before or after Ofgem opens any enforcement case.

Examples of aggravating factors which would tend to increase the penalty amount include:

- continuation of the contravention or failure after the OES becomes aware of it;
- the extent to which there is evidence that internal mechanisms and procedures as exist within the OES have not been properly applied and kept under appropriate review by senior management after becoming aware of the contravention or failure;
- any attempt to conceal all or part of a contravention or failure from Ofgem;
- failure to cooperate fully with reasonable requests from Ofgem's investigation team; and
- whether the contravention or failure was a repeat of a previous contravention or failure or part of a pattern of non-compliance.

Examples of mitigating factors which would tend to decrease the penalty amount would include:

- the extent to which the OES had taken steps to secure improved compliance either specifically or by implementing or updating an appropriate compliance policy, with effective management supervision;
- promptly, accurately and comprehensively reporting the contravention or failure to Ofgem that do not constitute a NIS incident;
- appropriate action by the OES to remedy the contravention or failure after becoming aware of it;
- evidence that the OES has taken steps to review its compliance activities and change them as appropriate in the light of the events that led to the investigation at hand; and
- providing co-operation with Ofgem's investigation that is well beyond what would be expected of any OES facing enforcement action, and goes well beyond, for example, merely meeting prescribed timescales for responding to Information Notices, or the requirement to co-operate with an inspection.

Step 4 – Consider an adjustment for deterrence

We will next consider whether a further adjustment to the penalty needs to be made within the identified penalty band to help ensure that it will have a sufficient deterrent effect. We may make such an adjustment if we consider that the penalty would otherwise be insufficient to deter the OES, or others, from committing further or similar contraventions or failures.

Step 5 – Establish the total financial liability

Having carried out the steps above we will consider the total financial liability of the OES and make any necessary final adjustments to ensure it is appropriate and proportionate to the contravention or failure in respect of which it is imposed. We may at this stage consider the effect of a proposed penalty on the financial viability of an OES and may make adjustments accordingly.

Any upward adjustments considered under steps 3, 4 or 5 are subject to the category maximums for a contravention or failure set out under Step 1.

Note on the meaning of Material Contravention

A Material Contravention is defined in regulation 18(7)(a) of the NIS Regulations. For the purposes of OES in the DGE sector, it means:

(i) a failure to take, or adequately take, one or more of the steps required under an Enforcement Notice within the period specified in that notice to rectify a failure described in one or more of regulation 17(1)(a) to (d); or

(ii) where an Enforcement Notice was not served or where no steps were required to be taken under an Enforcement Notice, a failure described in one or more of regulation 17(1)(a) to (d).

Regulations 17(1)(a) to (d) cover the following:

- failure to fulfil the security duties under regulations 10(1) and (2);
- failure to notify a NIS incident under regulation 11(1);
- failure to comply with the notification requirements stipulated in regulation 11(3) relating to NIS incidents; and
- failure to notify an incident as required by regulation 12(9).

Failures which are not treated as a Material Contravention will therefore generally include those relating to:

- failure to notify the Competent Authority under regulation 8(2);
- failure to comply with the requirements stipulated in regulation 8A relating to nomination by an OES of a person to act on its behalf in the UK;
- failure to comply with an Information Notice issued under regulation 15;
- failure to comply with a direction given under regulation 16(1)(c) in relation to an inspection;
- failure to comply with the requirements stipulated in regulation 16(3) relating to inspections; and
- failure to comply with the duty set out in regulation 17(3A) to comply with an Enforcement Notice.