Department for
Business, Energy
& Industrial Strategy

# BEIS Policy Guidance for the Implementation of the Network and Information Systems Regulations

## Government response to the public consultation

August 2022



Any enquiries regarding this publication should be sent to us at:
enquiries@beis.gov.uk

# Contents

# Executive Summary

The consultation ran from 04 October 2021 to 29 November 2021. In total, 19 responses were received from Operators of Essential Services (OES) and other stakeholders by email. 14 responses were from operators in the downstream gas and electricity (DGE) subsector, and five responses were from the oil and upstream gas subsector.

The consultation asked seven questions relating to the guidance document and the clarity of information provided in regard to the OES duties under the Network and Information Systems regulations (2018) (the NIS Regulations) and the Competent Authority implementation of the powers under the NIS Regulations.

Overall, respondents were supportive of the amendments to the BEIS policy guidance, stating that it improved clarity and transparency on the implementation of the NIS Regulations in the energy sector. Feedback from the consultation responses related mainly to:

- OES security duties
- Incident reporting
- Enforcement and penalty approaches

In addition, some responses included points relevant to the content of the NIS Regulations rather than the guidance. The purpose of the consultation was to seek feedback on the guidance. A consultation on the NIS Regulations has been held by the Department for Culture Media and Sport (DCMS) and responses to feedback received was issued [1].

[1] Government Response to the call for views on amending the Network and Information Systems Regulations, published 17 November 2021, available here.

# Background

The purpose of the consultation was to seek views on the updated guidance for the implementation of the NIS Regulations in the energy sector in Great Britain. There is no statutory duty to consult on the guidance. Views and comments were sought from persons designated as Operators of Essential Services (OES) and other relevant persons in the energy sector, to ensure the guidance is effective and appropriate for their needs.

The guidance published alongside this government response supersedes the previous guidance published in 2018 and is intended to support designated OES as defined by the NIS Regulations, and those yet to be designated OES, with ongoing compliance with their duties under the NIS Regulations. It is statutory guidance published under regulation 3(3) of the NIS Regulations; OES must have regard to it when carrying out their security duties under regulation 10. The guidance has been updated following a Statutory Instrument (SI) which made significant amendments to the NIS Regulations as a result of the findings from the first Post-Implementation Review of the NIS Regulations. Two further SIs[2] also came into force on 20 January 2021 following the UK's exit from the European Union. The updated guidance aims to provide greater clarity, consistency and transparency on the policies underpinning the implementation of the NIS Regulations in the energy sector. The guidance also sets out the Competent Authority approach to enforcement and penalties under the NIS Regulations.

This document summarises the responses received, the government's response and the main amendments to the guidance.

[2] The Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019, SI 2019/623, available here; and the Network and Information Systems (Amendment etc.) (EU Exit) (No. 2) Regulations 2019, SI 2019/ 1444, available here.

# Government Response

BEIS has considered all consultation feedback to the questions posed as well as the other comments submitted by respondents. A high-level summary of the responses is set out below, followed by the government response and summary of key amendments. As part of considering responses, some general amendments have been made to the guidance to improve clarity.

## Question 1: OES Roles and Responsibilities under the NIS Regulations

Feedback received showed that respondents were broadly satisfied that Chapter 4 of the guidance sufficiently sets out the roles and responsibilities of OES and yet to be designated OES under the NIS Regulations. However, there were a number of issues identified by respondents including:

### Compliance with security duties

Some respondents noted the reference to ‘compliance’ with NCSC Cyber Assessment Framework (CAF) security principles in paragraph 4.31 of the published draft and questioned the extent to which it adheres to the outcomes focused regulatory approach to the NIS Regulations.

**Government response**

The CAF is one of the tools used by the Competent Authority to assess compliance of OES who are in scope of the NIS Regulations. It provides Indicators of Good Practice against each element of the security principles devised by NCSC and provides a structured approach to assess the security and resilience of an OES’s network and information systems. We do not consider that the approach set out in the guidance contradicts the approach to the NIS Regulations. We have made some amendments to paragraphs 4.27 and 4.30 to add further clarity.

We have also clarified the situation regarding OES who are also subject to the Smart Energy Code (SEC).

### Duty to have regard to the State of the Art

Many respondents raised questions regarding the meaning of ‘state of the art’ and the requirement under the Regulations for OES to have “regard to the state of the art” when taking measures to ensure the level of security of network and information systems is appropriate to the risk posed. Respondents note that the NIS Regulations do not contain a definition for ‘state of the art’ and there were calls for BEIS to include a definition to assist in clarifying the benchmark for OES decision making when determining appropriate and proportionate security arrangements.

### Government response

We have included further considerations in paragraph 4.22 under Chapter 4 to assist OES in this area. However, 'state of the art' is not defined in the NIS Regulations, and it is not appropriate to give an exhaustive definition that may limit its meaning.

Chapter 4 of the guidance is a summary of the key duties of the OES and other parties who fall within the Scope of the NIS Regulations. Indeed, security risks, capabilities and approaches differ between OES; and operators must be able to consider the state of the art as it relates to their organisation.

## Scope of OES network and information systems captured within the NIS regulations

In Chapter 4, under the section titled '*identifying which network and information systems are in scope*,' some respondents suggested that the Competent Authority should formally accept the scope of the network and information systems identified by an OES of which network and information systems it relies upon, or which are used for the provision of an essential service. Respondents suggest there should be engagement with and acknowledgment of proposed systems in scope of the NIS Regulations, prior to any later enforcement action.

### Government response

OES are best placed to identify the systems which are in scope of the NIS Regulations. Nevertheless, the Competent Authority will continue to engage with OES where appropriate to ensure that OES have identified relevant network and information systems when they self-notify as being designated. We have included additional wording in paragraphs 4.33-4.39 to assist OES in identifying their network and information systems. Ofgem guidance[3] also contains relevant information.

## Notifying BEIS

Some respondents were of the opinion that the proposal in paragraph 4.14 of the original draft to provide information about a NIS Responsible Officer (NRO) to BEIS twice a year is burdensome, particularly as Ofgem and HSE have regular engagement with OES and should be in a position to attain this information.

Also, some respondents noted that the BEIS guidance did not contain a similar request in the draft Ofgem guidance (which was also open for consultation at the same time as the draft policy guidance) to include a NIS Accountable Officer.

### Government response

The ask for OES to report NRO information to BEIS twice a year has been removed. However, OES should inform BEIS if an OES undergoes any changes that BEIS should be aware of, such as changes of NRO details.

[3] NIS Directive and NIS Regulations 2018: Ofgem guidance for Operators of Essential Services

With regard to the NIS Accountable Officer role referred to in the Ofgem guidance; this role has been removed from the Ofgem guidance and contact information for this role will not be requested from OES by either BEIS or Ofgem. OES will only be requested to provide the information set out in paragraph 4.10 of the guidance.

## Question 2: Roles and Responsibilities of BEIS, Ofgem, and HSE

All of the respondents stated that the roles of BEIS and Ofgem as joint Competent Authorities in the downstream gas and electricity subsector was clearly set out in the guidance. Similarly, respondents' feedback was that the compliance functions carried out by HSE in relation to the oil and upstream gas subsector is sufficiently set out in the guidance. A few respondents did highlight the need to ensure alignment in the NIS Regulations' implementation across the energy sector.

### Government response

The roles of BEIS, Ofgem and HSE are clearly defined and communicated. BEIS liaise closely with Ofgem and HSE to ensure a consistent approach across the sector, where appropriate.

## Question 3 and 6: Incident Reporting template and Voluntary Incident Notification

Overall, there were few substantive comments on the incident reporting template. Respondents found the voluntary incident notifications guidelines at Annex F of the guidance clearly presented and useful.

Some respondents requested clarity on the details of mandatory and voluntary reporting covered in the guidance. Some also stated that there were several organisations referred to as points of contact for incident reporting and sought a single point of contact for incident reporting. One respondent stated that the government was requesting numerous reports at a time when the OES will be focused on managing the incident.

### Government response

We consider that the guidance contains clear information regarding the mandatory NIS Incident reporting requirements. Similarly, we think that the guidance is also clear about when the OES may submit voluntary incident reports for other incidents which do not meet the requirements under regulation 11 of the NIS Regulations. Voluntary incident reporting is encouraged to allow OES to access support from NCSC and BEIS as appropriate, as well as to alert government of any potential impacts on essential services.

We have included separate paragraphs on mandatory and voluntary incident reporting in Chapter Four to add further clarity as to OES duties under the NIS Regulations and those

matters which are voluntary. We have also clarified the single points of contact for OES to submit mandatory incident reporting at paragraph 4.47.

Voluntary incident reports should go to the NCSC with the template submitted at Annex F, and OES also have the option of contacting the BEIS Emergency Response, Capabilities and Operations team for support with incident response as appropriate. To clarify, as stated in the guidance at paragraph 4.55 the OES is responsible for incident response.

We have included a note to Annex E to provide further guidance on what is meant by the 'Type of Incident' in response to query about the meaning of non cyber incidents. We have accordingly removed this term from the guidance.

# Questions 4 and 5: Competent Authority Enforcement Powers and Penalty Policy

Overall, respondents were generally supportive of the information provided on enforcement process. They stated that the guidance is straightforward and will support stakeholder understanding.

However, some themes emerged in the consultation responses which can be characterised broadly as requests for further information and clarity.

## Inspections

Reponses were received in relation to the subsection titled 'Power of Inspection' under Chapter Five of the guidance. Feedback received suggested concern regarding the powers that inspectors have 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 OES's main objective to secure and restore service during a cyber incident. Respondents suggest that any direction from the Competent Authority in such circumstances could delay restoration and increase security risk.

Some respondents asked that an inspector's power to conduct tests or direct OES to conduct tests should be further clarified, reduced in scope or removed altogether.

Furthermore, some respondents also wanted assurance on issues such as suitable confidentiality and security arrangements being in place before inspections occur. In addition, it was suggested there should be means for verifying the identity of inspectors before they could enter the premises.

Finally, a respondent considered that suspected non-compliance should be a pre-requisite for inspections for compliance or enforcement purposes.

### Government response

Chapter five of the guidance summarises the enforcement powers available to Competent Authorities under the NIS Regulations and the usual Competent Authority approach to enforcement. Many of the relevant consultation responses were essentially about the content of the NIS Regulations rather than the guidance. With regards to clarifying that suspicion of non-compliance is a pre-requisite for compliance or enforcement focused inspections, the Competent Authority will comply with the requirements of the NIS Regulations in relation to inspections, but do not consider that suspicion of non-compliance is required to conduct an inspection (though suspicion of non-compliance could be a situation in which an inspection might be appropriate).

With regards to the powers inspectors have under the NIS Regulations, we believe that the NIS Regulations contain appropriate safeguards. For example, regulation 16(7) requires inspectors to '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'.

The NIS Regulations confer the power on inspectors to conduct or direct OES to conduct tests pursuant to regulation 16(5)(f). The guidance reflects the power of inspection as provided for in the NIS Regulations and so changes would not be appropriate.

On ensuring the identity of inspectors, it is worth noting paragraph 5.17 which clarifies that inspectors will have regard to the Code of Practice on Powers of Entry, issued by the Home Office. In terms of security concerns about inspectors and any issues about interference with OES's ability to undertake their duties under the NIS Regulations, we consider there are appropriate safeguards in the NIS Regulations. regulations 16(6), 16(7), and 16(8) place various requirements on inspectors such as presenting identification at premises on request, and keeping material, documents, information, or equipment removed secure from unauthorised access, interference, and physical damage.

## Penalty Approach

Respondents were generally supportive of the NIS penalty approach in chapter five. Stakeholders believed the structure was relatively clear and that the process would help provide clarity and transparency around the factors that would normally be considered when determining the amount of a financial penalty under the NIS Regulations.

However, feedback on the approach to penalties also reflected a desire from respondents 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.

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. One respondent called for the incorporation of a 'quantitative methodology' to help improve the policy.

Other comments regarding the NIS penalty approach 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 and this should be taken into consideration as mitigation when making any penalty assessment. Another respondent mentioned that some OES might be financially at risk and a penalty could increase that risk, so calculations should take that into account. One respondent requested the inclusion of process flowcharts with estimates of the likely timelines for cases.

A respondent also stated that the process to ensure that the facts and any circumstantial evidence is collected from the OES appears to be missing from this overall NIS penalty approach.

### Government response

The NIS penalty approach must of course reflect the requirements of the NIS Regulations. We intend to create a reliable, repeatable, and transparent framework within which each case can be considered on its merits.

The term “material contravention” in defined in regulation 18(7) and the guidance refers to this. The NIS Regulations and guidance set out how determining whether a contravention is material (or not) will determine 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.

The NIS penalty approach includes a step (Step 5) that allows for an adjustment to be made to take account of OES financial circumstances. 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. It is possible that a contravention or failure caused by a larger OES, serving more consumers, has a greater potential to harm consumers or other market participants (other things being equal).

Regarding whether an OES might be a victim of crime, potentially by a state actor, we consider that ‘Step 2’ of the penalty policy can consider such matters. ‘Step 2’ provides that the Competent Authority may consider ’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.

## Other responses

### Duplicative enforcement

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 set out in guidance.

Regarding special arrangements to assist consistency across sectors or across international borders, we consider these matters are beyond the scope of this guidance. 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 Competent Authority for OES that operate across sectors, is necessary.

## Information sharing

A few respondents mentioned information sharing by the Competent Authority and one respondent requested that the relevant OES should be contacted to make representation on the sharing of such information.

The Government considers that NIS Regulations contain adequate safeguards in relation to information sharing. Regulation 6(1) sets out the circumstances in which Competent Authorities and the Information Commissioner may share information with each other, relevant law-enforcement authorities, the NCSC, and public authorities in the EU. Furthermore, regulation 6(1A) imposes further requirements on information sharing, stating, namely that information shared under regulation 6(1) may not be further shared by the person with whom it is shared for any purpose other than mentioned in regulations 6(1) unless otherwise agreed by the NIS enforcement authority. Regulations 11(8) also includes a duty to consult when an incident is proposed to be published.

This publication is available from: www.gov.uk/beis

If you need a version of this document in a more accessible format, please email enquiries@beis.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.