Department for
Business, Energy
& Industrial Strategy

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

for the Energy Sector in Great Britain

Closing date: 29 November 2021

October 2021

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

Contents

Foreword

The purpose of this consultation is to:

- set out the proposed updates to the BEIS Policy Guidance for the Implementation of Network and Information Systems Regulations in Great Britain (GB) energy sector following amendments to the Network and Information Systems Regulations 2008 ("the NIS Regulations"); and

- provide an opportunity for stakeholders to put their views and comments to the Department for Business Energy and Industrial Strategy so that they can be considered as part of the NIS implementation process.

Consultation details

Issued: 04 October 2021

Respond by: 29 November 2021

Enquiries to:

Energy Cyber Security, Regulatory Policy Team
Department for Business, Energy and Industrial Strategy
3rd Floor
1 Victoria Street
London
SW1H 0ET

Email: nis.energy@beis.gov.uk

Consultation reference: Consultation on the BEIS Policy Guidance for the Implementation of the Network and Information Systems Regulations for the Energy Sector in Great Britain.

Audiences:

The Government seeks views from persons designated as Operators of Essential Services (OES) under the NIS Regulations in the energy sector in Great Britain, as well as other relevant persons (e.g., professional bodies, other energy companies) in the energy sector.

Territorial extent:

Great Britain. The proposed guidance does not apply to Northern Ireland.

How to respond

We welcome your views. We encourage respondents to make use of the online e-consultation where possible when submitting responses as this is the government's preferred method of receiving responses. However, responses via email will also be accepted. Should you wish to submit your main response via the online platform and provide supporting information via email, please be clear that this is part of the same response to this consultation.

Below are the methods for submitting a response:

By Email to:

nis.energy@beis.gov.uk

By Post:

Regulatory Policy Team, Energy Cyber Security
Department for Business, Energy and Industrial Strategy
3rd Floor
1 Victoria Street
London
SW1H 0ET

When responding, please state whether:

- you are responding as an individual or representing the views of an organisation;
- you are willing to be contacted (if so, please provide contact details); and
- you prefer for your response to remain confidential and non-attributable (if so, please specify).

Your response will be most useful if it is framed in direct response to the questions posed, though further comments and evidence are also welcome.

Confidentiality and data protection

Information you provide in response to this consultation, including personal information, may be disclosed in accordance with UK legislation (the Freedom of Information Act 2000, the Data Protection Act 2018 and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential, please tell us, but be aware that we cannot guarantee confidentiality in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not be regarded by us as a confidentiality request.

We will process your personal data in accordance with all applicable data protection laws. See our privacy policy.

We will summarise all responses and publish this summary on GOV.UK. The summary may include the names of organisations that responded, but not people's personal names, addresses or other contact details.

Quality assurance

This consultation has been carried out in accordance with the government's consultation principles.

If you have any complaints about the way this consultation has been conducted, please email: beis.bru@beis.gov.uk.

Executive summary

The Network and Information Systems Regulations 2018 ("the NIS Regulations") provide legal measures aimed at improving the protection of the network and information systems that are critical for the delivery of the UK's essential services including transport, energy, water, health and digital infrastructure sectors as well as to online marketplaces, online search engines and cloud computing services (as digital service providers).

Competent Authorities (CAs) are responsible for the oversight of compliance with the NIS Regulations in each sector. In accordance with the NIS Regulations[1], CAs must prepare and publish guidance in relation to their sector. This guidance may be published in such form and manner as the CA considers appropriate and reviewed at any time.

For the energy sector the CAs, as named in the NIS Regulations, are the Secretary of State for the Department of Business, Energy and Industrial Strategy ("BEIS") for the oil subsector and the gas subsector in relation to upstream gas[2], and Ofgem and BEIS acting jointly for the electricity subsector[3] and gas subsector in relation to downstream gas[4]. HSE undertakes certain compliance and enforcement functions for the oil sector and specified sections of the gas sector on behalf of BEIS.

BEIS published guidance for the implementation of the NIS Regulations in the energy sector for Great Britain[5] in July 2018. This guidance explained the NIS Regulations and the requirements on Operators of Essential Services. The guidance also included instructions for the handling of incident notifications and was focused on the initial years of the NIS Regulations.

In May 2020, the Government published its first Post-Implementation Review of the NIS Regulations. The review's purpose was to evaluate how effective the NIS Regulations have been in achieving their original objective of improving security standards. The review showed that, whilst it is still too early to judge the long-term impact of the NIS Regulations, organisations in scope (operators of essential services, or OES) are beginning to take steps to improve the security of their network and information systems and that the NIS Regulations are having a positive effect. The Post-Implementation Review also identified several areas of

[1] Regulations 3(3)(b) of the NIS Regulations
[2] Upstream gas' refers to the essential services within the gas sub-sector specified in Schedule 2, paragraph 3, sub-paragraphs (5) to (8) of the NIS Regulations
[3] The 'electricity' sub-sector refers to the essential services specified in Schedule 2, paragraph 1 of the NIS Regulations.
[4] Downstream gas' refers to the essential services within the gas sub-sector specified in Schedule 2, paragraph 3, excluding sub-paragraphs (5) to (8) of the NIS Regulations.
[5] Security of Network and Information Systems Regulation 2018: implementation in the energy sector for Great Britain, available here.

improvement to the NIS Regulations requiring policy interventions from the Government, which would enhance their overall efficiency. These relate to:

- introducing an independent appeal mechanism;
- changes to regulatory authorities' enforcement powers;
- expanded information-sharing provisions;
- amendments to the threshold requirements for deemed designation by OES; and
- refining the application of penalties, and other technical and operability changes.

On 31 December 2020, an SI came into force which made significant amendments to the NIS Regulations as a result of the findings from the first Post-Implementation Review of NIS. Two further SIs[6] also came into force on 20 January 2021 following the UK's exit from the EU.

This proposed revised version of the guidance is intended to supersede the previous guidance and is intended to support OES with on-going compliance with the NIS Regulations. The proposed guidance has been updated by BEIS to reflect the amendments made by the 2020 SI to the NIS Regulations and sets out how the CA function will be carried out under the NIS Regulations in the energy sector in Great Britain.

The updates to the guidance specifically relate to:

- enforcement;
- penalties;
- appeals; and
- inspections.

We are seeking views from those OES to which the guidance applies, and any other relevant persons in the energy sector. The purpose of this consultation is to establish whether the proposed guidance provides appropriate support to assist OESs in complying with the NIS Regulations, and to determine the impact of the proposed new procedures on OES.

[6] 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.

Proposed BEIS Policy Guidance

The government intends to publish the proposed revised BEIS Policy Guidance for the implementation of the NIS Regulations in the GB energy sector. The proposed BEIS Policy Guidance is published alongside this consultation. The guidance has been updated to reflect the amendments made by the 2020 SI to the NIS Regulations. It contains seven chapters.

Chapter 1 and 2 - The NIS Regulations

Chapter 1 – About this document.

This chapter provides an overview of the guidance namely, to aid entities that are designated, or yet to be designated as OES in the energy sector in understanding their duties under the NIS Regulations as well as the duties of the CA in relation to oversight, compliance, and enforcement and how these will be carried out.

Chapter 1 has been updated to include reference to the amendments made by the 2020 SI to the NIS Regulations. It reflects the current provisions in relation to:

- enforcement;
- penalties;
- appeals; and
- inspections.

Chapter 2 provides information on the background to, and the development of the NIS Regulations and its implementation in the UK energy sector. The chapter provides background to the NIS Directive (which formed the basis of the UK NIS Regulations) and has been updated to include the implications of the UK's departure from the EU on the NIS Regulations and cybersecurity regime more generally.

Further, it explains the roles of the National Cyber Security Centre (NCSC) under the NIS Regulations as the Computer Security Incident Response Team (CSIRT) and the Single Point of Contact (SPoC).

Chapter 2 also includes information on the principles which OES are expected to meet to manage the security of their network and information systems. Finally, it contains information on the cyber assessment framework (CAF) which is used to assess compliance for OES.

Chapter 3 - Implementation of the NIS Regulations in the Energy Sector in Great Britain

Chapter 3 provides guidance on the implementation of the NIS Regulations for designated OES and prospective OES. This section of the guidance remains largely the same as the existing BEIS policy guidance and sets out the roles and responsibilities of BEIS, Ofgem and HSE as the CAs. This chapter sets out the key responsibilities of the CAs in the oversight, compliance, and enforcement of the Regulations, and BEIS collaboration with OES on cyber resilience issues outside of the NIS Regulations.

Over time the cyber security landscape is evolving, for instance the recently published Smart Systems and Flexibility plan highlights the emerging role of 'load controllers' in the energy system. Chapter 3 sets out BEIS role in keeping pace with developments such as these, in the context of the NIS Regulations

The chapter is updated to reflect amendments made by the 2020 SI to information sharing provisions which provide further clarification as to how CAs can share information with each other, and with law enforcement authorities for regulatory and national security purposes and for the purpose of criminal proceedings and investigations.

Chapter 4 - Duties on OES

OES are subject to the requirements of the NIS Regulations. Chapter 4 provides an overview of the key duties of OES (as well as those yet to be designated as OES) and other parties who may fall within the scope of the NIS Regulations.

The chapter includes information on the OES' duty to:

- notify the CA in relation to their designation under the NIS Regulations
- take measures to manage risks to the security of networks and information systems, and to prevent and minimise the impact of incidents
- notify the CA of incidents which meet the thresholds in the guidance
- comply with instructions and directions for the purpose of inspections under the NIS Regulations
- comply with Information Notices, Enforcement Notices and Penalty Notices; and
- pay the reasonable costs incurred by CAs in carrying out functions under the NIS Regulations.

Designation and Revocation

This section of the guidance contains information on the CAs designation and revocation powers under the NIS Regulations and the information that will be required from operators to confirm their designation as OES.

The Statutory instrument amending the NIS Regulations[7] introduced a duty for OES based outside the UK to nominate a person to act on its behalf in the UK. Thus, chapter 4 discusses the requirement on entities that provide an essential service in the UK but have a head office outside of the UK to nominate a person in the UK to act on their behalf under the NIS Regulations within 3 months of coming into scope of the NIS Regulations.

Security Duties

The guidance on security duties has been revised to provide greater clarity on the expectations of OES in ensuring the security of their network and information systems. Furthermore, this section of the guidance makes it clear that OES are expected to utilise the NCSC CAF to demonstrate compliance with the security duties under the NIS Regulations.

Incident notification

This section of the guidance contains details on the incident reporting duties of OES, and the notification procedures for the purposes of complying with the NIS Regulations. Specifically, it discusses:

- the definitions and thresholds that OES need to consider when determining whether an incident must be notified under the NIS Regulations; the incident notification thresholds in Annex C of the guidance are provided as guide to establish whether an incident has a significant impact on the continuity of the essentials service.
- the incident notification procedures for mandatory incident notification and voluntary incident notification. These procedures should be considered with Annex C of the guidance which provides the incident notification template for mandatory incident notification; Annex E of the guidance, which provide guidelines for notifying incidents voluntarily to the NCSC.

The incident reporting thresholds are concerned with the continuity of essential services, however the Government is conscious that there may be events which do not affect the continuity of the essential service, but may affect the network and information systems that the essential service relies on.

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

As such, we are consulting on lowering the incident notification thresholds because OES are yet to experience any incident affecting networks and information systems with a significant impact on the continuity of the essential service since the NIS Regulations came into force in 2018.

Incident information is invaluable for the Government to understand the threats affecting the energy sector, and to identify thresholds that could inform our implementation of the NIS Regulations. Hence, lowering the incident notification thresholds will allow the Competent Authority to receive data that may be useful in improving the effectiveness of the NIS Regulations.

Chapter 5 – Competent Authority Approach to Enforcement, Compliance and Penalties. Requirements on Operators of Essential Services

Enforcement of the NIS Regulations is the responsibility of the designated CA. Chapter 5 sets out the approach of BEIS, Ofgem and HSE to carrying out their duties under the NIS Regulations and subsequent Agency Agreement[8] (in the case of HSE) and enforcing the NIS Regulations in the energy sector in Great Britain. Ofgem have also produced an updated enforcement guidance which they will also be consulting on. To note, this implementation approach is specific to the GB energy sector.

Information requests by the Competent Authority

This section of the guidance covers the circumstances in which the CA may serve an Information Notice on an OES. It reflects the changes introduced by the 2020 SI which expanded the purposes for which Information Notices could be served to include to establish whether there have been any events that had an adverse effect on networks or information systems. This amendment allows the CA to identify failures to comply with the duties in the NIS Regulations and ensures it has access to relevant information in relation to breaches in order to make informed decisions before proceeding to enforcement or penalty action. Information Notices can also be a useful tool for CA to obtain information on near-miss incidents which do not meet the threshold for incident reporting under the NIS Regulations, but which could provide the CA with useful insight on the cyber threats faced by the GB energy sector.

Power of Inspection

The CAs will conduct inspections to ensure compliance with the requirements of the NIS Regulations. This section of the guidance sets out the inspection powers available to the CA and some of the duties of the OES in relation to inspections. For example, the OES will be

[8] Agency Agreement between HSE and BEIS available here.

required to comply with any requests made by, or requirement of, an inspector performing their functions under the NIS Regulations, and to comply with any requests to pay the reasonable costs for an inspection.

Ofgem and HSE have produced further guidance detailing the inspection frameworks in the subsectors (or aspects of subsectors) within their respective remit. In the gas subsector in relation to downstream gas and the electricity subsector, Ofgem have published a NIS Inspection Framework and HSE conducts inspections in the oil subsector and gas subsector in relation to upstream gas on the basis of their OG86 operational guidance[9].

Enforcement Notices

The CA may rely on the enforcement powers in the NIS Regulations to ensure that OES have appropriate and proportionate security measures in place and that they fulfil their obligations under the NIS Regulations. The section of the guidance sets out the enforcement powers, in particular the circumstances in which the CA may issue an Enforcement Notice. It details the right of an OES to submit representations before an Enforcement Notice is served and the duty on the OES to comply with the requirements of an Enforcement Notice.

The section of the guidance reflects the changes introduced by the 2020 SI, and to clarify that the CA may serve multiple enforcement notices where it would be appropriate and proportionate to do so (e.g., where the CA needs to address more than one breach simultaneously).

Penalty Notice

The CA has the power to impose substantial financial penalties, if necessary. This section of the guidance covers the following:

- when a penalty can be issued
- what actions the CA must take before issuing a Penalty Notice
- the considerations that the CA must take into account when issuing a Penalty Notice
- the steps in determining the penalty amount
- the potential for the CA to commence civil proceedings against an OES, for failure to comply with an Enforcement Notice.

An Enforcement Notice need not be issued before a Penalty Notice is issued. Furthermore, guidance is provided on the two-step process introduced in the Regulations, whereby the CA may serve a notice of intention to impose a penalty before making the final decision, allowing OES to submit representations before the CA issues a formal Penalty Notice.

[9] HSE OG86 Operation Guidance available here

The Guidance has been updated to reflect the revised penalty categories which have been amended to reflect the seriousness of different categories of breaches. The CA has the discretion to issue penalties to reflect the seriousness of the breach, and the section sets out the considerations for the CA in determining the amount of the penalty.

In the energy sector, BEIS is responsible for issuing penalties for contraventions of an OES's NIS duties in the oil subsector and gas subsector in relation to upstream gas, whilst Ofgem is responsible for penalties in the gas subsector in relation to downstream gas and the electricity subsector. As such, Ofgem will issue further guidance on their enforcement process including penalties.

General Enforcement Considerations

This section of the guidance sets out the general considerations which the Competent Authority will consider when taking enforcement action against an OES.

Disclosure of Notices

In carrying out the enforcement duties under the NIS Regulations, the Government is committed to being fair and transparent and as visible as possible in the actions that we take. This section of the guidance sets out the CAs' intention to make Enforcement and/or Penalty Notices public where possible. This will be considered on a case-by-case basis, and we will take into account national security and confidentiality issues.

Enforcement by Civil Proceedings

This section of the guidance sets out the new powers of the CA to initiate civil proceedings against an OES in addition to, or instead of a Penalty Notice, if they fail to comply with the requirements of an Enforcement Notice.

Informal Resolution

There are some circumstances where a breach or a contravention has occurred, the CA may seek informal resolution to bring an OES into compliance and remedy the consequences of the failure or breach. This section of the guidance sets out the informal actions which may be agreed to, as well as the considerations of the CA before the CA may agree to any informal action to resolve a failure or contravention.

Chapter 6 - Appeals

Previously, CAs were required to appoint an independent reviewer at the request of an OES to review either designation decisions or decisions to issue Penalty Notices. The 2020 SI amended the NIS Regulations to introduce an appeals mechanism to ensure consistency of the application of the Regulations across sectors and to limit the burden on OES and CAs. OES can now seek redress through a statutory appeals process with appeals heard by the General Regulatory Chamber of the First-Tier Tribunal. This chapter sets out that the decisions that an OES may appeal to the First-tier Tribunal, the grounds for the appeals and the potential outcomes of the appeal process.

The appealable matters under the NIS Regulations have been expanded to include enforcement notices and revocation of designation notices, in addition to designation notices and penalty notices. The appeals mechanism provides OES with more flexibility to raise appropriate appeals.

The guidance has been updated to reflect these changes.

Consultation questions

We invite respondents' considerations, where possible with appropriate evidence, on the proposed revised BEIS Policy Guidance. We specifically invite responses to the following questions:

1. Does the guidance sufficiently set out the roles and responsibilities of designated OES, and not-yet-designated persons under the NIS Regulations? Please set out any additional information or questions that you require to further understand those duties.

2. Do you clearly understand the roles and responsibilities of BEIS, Ofgem and HSE in the energy sector? If not, please set out what additional information will aid your understanding.

3. Regarding the incident notification template at Annex D of the guidance, are there any changes you would propose to improve the template. If yes, please provide information and evidence.

4. Does Chapter 5 of the guidance provide clear information regarding the actions that the CA may take to enforce the duties under the NIS regulations? If no, please detail what changes may be helpful?

5. Are the processes for serving a Penalty Notice and for determining the sum of a penalty sufficiently clear? Is there any aspect of this section that require further detail or explanation?

6. Are the voluntary incident notification guidelines in Annex E of the guidance clearly presented? Is there any further information that you require?

7. Is there any other information not currently covered in the guidance that would be beneficial to include? Please specify.

Next steps

The Government will publish a response to this consultation on the GOV.UK website, summarising the received responses and setting out the actions that will be taken in developing our final version of the BEIS Policy Guidance. The consultation response will be published within three months of the consultation closing.

The final BEIS Policy Guidance will be published thereafter and will replace the guidance entitled ‘Security of Network and Information Systems Regulations 2018: implementation in the energy sector for Great Britain’ that was published on 2nd July 2018.

This consultation is available from: www.gov.uk/government/consultations/implementation-of-the-network-and-information-systems-regulations-in-the-energy-sector-amendments-to-guidance

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.