Department for
Business, Energy
& Industrial Strategy

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

for the Energy Sector in Great Britain

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

Contents

Chapter 1 - About this document

1.1. This guidance is intended to help designated Operators of Essential Services (OES), and yet-to-be-designated persons (i.e., legal entities) in the energy sector in Great Britain (GB) in complying with the Network and Information Systems Regulations 2018 ("the NIS Regulations").

1.2. This document summarises the duties on OES as well as the roles and responsibilities of the Competent Authorities (the bodies responsible for oversight, compliance, and enforcement of the NIS Regulations within a sector) and how these will be carried out. It also sets out the process and thresholds for NIS incident notifications.

1.3. Energy is a reserved matter in Scotland and Wales and is devolved in Northern Ireland. The guidance therefore covers England, Scotland and Wales, but not Northern Ireland. OES in Northern Ireland should refer to their Competent Authority, as set out in Schedule 1 to the NIS Regulations, for further information.

1.4. This document has been provided to answer key questions that organisations may have, including:

- How the NIS Regulations are implemented within Great Britain
- Which organisations are in scope of the NIS Regulations;
- Who the Competent Authorities are for the energy sector in Great Britain;
- The roles and responsibilities of the Department for Business, Energy and Industrial Strategy (BEIS), the Office of Gas and Electricity Markets (Ofgem), the Health and Safety Executive (HSE) and the National Cyber Security Centre (NCSC);
- The Competent Authority approach to enforcement and penalties under the NIS Regulations;
- The responsibilities of OES;
- The requirements for incident reporting and;
- Cyber and non-cyber incident response, including instructions on how OES should contact NCSC to receive support.

1.5. This guidance is part of a wider collection of guidance available to OES in the energy sector in Great Britain; Ofgem and the HSE have developed their own

guidance to support OES in ensuring compliance with the NIS Regulations including[1]:

- guidance on their respective enforcement approaches and inspection frameworks;
- details of the Competent Authorities' approach to working with OES from identification of critical systems to OES assessment of their current security practices, assessment of risk, development of improvement plans and where required, monitoring and continuous improvement; and
- further information about handling incident reporting, response, and recovery

1.6. OES should ensure they have obtained any legal or professional advice necessary to ensure compliance with their duties under the NIS Regulations. This guidance:

a) does not create any rights enforceable at law in any legal proceedings;

b) is not a substitute for legal advice;

c) is not a set of binding instructions, although it includes references to provisions in the NIS Regulations which are statutory requirements;

d) does not limit the right of relevant Competent Authorities to make their own judgement or establish their own processes in accordance with the NIS Regulations. Competent Authorities are not bound to follow this guidance and may depart from it in appropriate circumstances; and

e) will be interpreted in line with any future amendments to the NIS Regulations.

1.7. This Guidance has been updated to reflect amendments made to the NIS Regulations 2018 by Statutory Instruments[2]: It reflects the current NIS Regulations and includes new or amended statutory provisions in relation to:

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

[1] Further information on the wider collection of NIS guidance in the energy sector is at Annex A.
[2] 2018/629, 2019/653, 2019/1444, and 2020/1245

Chapter 2 - Background

Background to and development of the NIS Regulations

2.1. The NIS Regulations came into force on 10 May 2018 and are aimed at improving the protection of the network and information systems[3] that are critical for the delivery of the UK's essential services including transport, energy, water, health, and digital infrastructure services as well as to online marketplaces, online search engines, and cloud computing services (as digital service providers).

2.2. OES in the transport, energy, water and health subsectors including digital infrastructure services (including online marketplaces, online search engines and cloud computing series) are required to demonstrate active cyber security risk management, report incidents that disrupt the continuity of the service and take action to rectify those incidents. The NIS Regulations identify a role for one or more regulatory bodies ('Competent Authorities') to ensure compliance. This regulatory activity is further supported by the UK's technical authority, the National Cyber Security Centre (NCSC).

2.3. The NIS Regulations are the transposition of the EU Security of Network and Information Systems Directive[4] (NIS Directive) into national legislation. The NIS Directive was adopted by the European Parliament in 2016. Its aim was to provide measures to:

a) ensure that Member States have in place a national framework — consisting of one or more Competent Authorities and one or more Computer Security Incident Response Teams (CSIRTs) — to support and enforce appropriate and proportionate levels of security of network and information systems; and

b) promote co-operation among all the Member States, by setting up a Co-operation Group to support and facilitate strategic cooperation, as well as a CSIRT Network to promote effective operational cooperation on specific network and information system security incidents and as well as the sharing of information about risks.

2.4. As of 1 January 2021, the UK is no longer an EU Member State. However, the Government decided to retain the NIS Regulations to ensure there is no gap in the regulatory regime after the withdrawal of the UK from the EU. The NIS Regulations were amended to change provisions that were inappropriate or redundant as a result of the withdrawal of the UK from the EU. Amendments include the removal of obligations on UK competent authorities to liaise, co-operate and share information with the European Commission and authorities in EU Member States. Co-operation and information sharing can still occur where appropriate. These amendments came into force on 31st December

[3] Regulation 1(2) of the NIS Regulation provides the meaning of network and information systems.
[4] The Security of Network and Information Systems Directive, available here.

2020, at the end of the transition period[5] to ensure that there is no gap in the regulatory regime after the withdrawal of the UK from the EU.

2.5. The NIS Regulations form part of the Government's National Cyber Strategy[6] to protect the UK in cyber space and make the UK the safest place to live and work online.

2.6. In 2020, the European Commission reviewed the functioning of the NIS Directive. Following this review, the European Commission published the proposals for a new directive, known as the NIS 2.0 Directive on 16 December 2020. The proposed NIS 2.0 Directive will repeal the NIS Directive and introduce amendments to expand on the scope of the application to additional sectors and services, adjust requirements and enforcement mechanism, and support cooperation at the European level. As the UK is no longer a Member State of the European Union, it is under no obligation to implement the NIS 2.0 Directive and may diverge from the EU approach in future iterations of the NIS Regulations.

2.7. If you have any questions about the NIS Regulations in general, please contact the DCMS NIS policy team at nis@dcms.gov.uk.

2.8. Schedule 1 to the NIS Regulations designates Competent Authorities for specified sectors and subsectors. Within the energy sector specified by Schedule 1 are specified subsectors relating to electricity, oil and gas. One or more competent authorities are designated for each subsector.

2.9. For the oil subsector[7][8] in Great Britain, the Competent Authority is the Secretary of State for BEIS

2.10. For upstream gas[9] services within the gas subsector in Great Britain, the Competent Authority is the Secretary of State for BEIS.

2.11. For downstream gas[10] services within the gas subsector in Great Britain, the Competent Authorities are the Secretary of State for BEIS and Ofgem[11] acting jointly.

2.12. For the electricity subsector[12] within Great Britain, the Competent Authorities are the Secretary of State for BEIS and Ofgem acting jointly.

---

[5] Explanatory Memorandum for the 2020 SI No. 1245, available here.
[6] Available here
[7] The NIS 2 Directive is available here
[8] The threshold requirements for essential services in the 'oil subsector' are specified in Schedule 2, paragraph 2 of the NIS Regulations.
[9] '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.
[10] '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.
[11] The body designated in the NIS Regulations is the Gas and Electricity Markets Authority (GEMA). Ofgem is a non-ministerial government department and carries out the day-to-day work of GEMA. Ofgem and GEMA are used inter-changeably in this document.
[12] The 'electricity' sub-sector refers to the essential services specified in Schedule 2, paragraph 1 of the NIS Regulations.

2.13. In addition, HSE will undertake certain compliance and enforcement functions for the oil sector and the upstream gas sector on behalf of BEIS. Chapter 3 sets out more detail on roles and responsibilities of these bodies. References to "the Competent Authority" in this guidance mean Ofgem and BEIS, or HSE acting on behalf of BEIS.

2.14. In the upstream gas and oil subsectors, BEIS and HSE have incorporated the NIS Regulations into the regulatory approach under the Control of Major Accident Hazards (COMAH) Regulations and the Offshore Safety Directive (OSD) to minimise the burden on OES.

2.15. The UK Government is committed to ensuring that the implementation of the NIS requirements:

- is realistic and proportionate to the risks that the requirements are intended to address
- follow outcome-based security principles
- provide flexibility to be delivered with industry ownership, HMG support and appreciation of industry perspectives
- reflect transition and build up over several years.

2.16. The Secretary of State for Digital, Culture, Media and Sport[13] (DCMS) is the Government Minister responsible for administering and maintaining the NIS Regulations. DCMS is responsible for reviewing them periodically[14] and introducing regulatory amendments, when necessary.

2.17. Two years after the NIS Regulations came into force, DCMS conducted a Post-Implementation Review that was published in May 2020[15]. The review concluded that the NIS Regulations had led to improvements in the security of the networks and information systems of the OES in scope and identified areas of improvement requiring further policy interventions from the Government and amendments to the NIS Regulations.

2.18. As a result, the Government introduced additional amendments to the NIS Regulations that came into force on 31st December 2020[16]. These amendments were informed by the feedback received during the Call for Views[17] and the findings of the 2020 post-Implementation review. An overview of the amendments introduced by the statutory instrument is available here.

[13] DCMS site on the NIS Regulations, available here.
[14] The Post-Implementation Review of the NIS Regulations is a statutory requirement under Regulation 25 of the NIS Regulations.
[15] Review of the Network and Information Systems Regulations, available here.
[16]The Network and Information Systems (Amendment and Transitional Provisions etc.) Regulations 2020. SI No. 1245, available here.
[17] Call for Views on proposed amendments to the NIS Regulations, available here.

The National Cyber Security Centre (NCSC)

2.19. The NIS Regulations name the Government Communications Headquarters (GCHQ) as the UK's Computer Security Incident Response Team (CSIRT)[18] and single point of contact (SPOC)[19]. The NCSC, a part of GCHQ, carries out these functions.

2.20. The NCSC plays several critical roles in support of the implementation of the NIS Regulations. As the CSIRT, the NCSC is responsible for: incident response, including monitoring incidents; providing dynamic incident analysis and situational awareness; providing early warning alerts as well as announcements and dissemination of information to relevant stakeholders about threats, risks, and security incidents. However, NCSC is not a substitute for the incident management function in an OES and the level of assistance they will provide depends on the impact and cause of the incident. Chapter 4 sets out more detail on incident reporting.

2.21. As the SPOC, the NCSC acts as liaison on NIS Directive matters between the UK and the EU and between different Competent Authorities. The role includes preparing a summary report of incident notifications and liaising with relevant authorities in EU Member States on incidents with potential cross-border ramifications.

2.22. The NCSC is also the UK technical authority on cyber security and in this capacity continues to support both the Competent Authorities and OES by providing technical expertise. In support of the NIS Regulations specifically, this includes developing a set of cyber security principles[20], a collection of supporting guidance[21] and assessment tools.

2.23. All these roles are advisory; the NCSC does not have regulatory responsibilities, and will not be able to, or seek to, enforce any actions on an OES or endorse any OES specific activities. Enforcement is solely the responsibility of Competent Authorities.

The NIS Cyber Security Principles and Guidance Collection

2.24. This comprises a set of outcome-based security principles which OES are expected to meet to manage the security of their network and information systems. These are underpinned by a suite of additional guidance which provides further information on how an OES may achieve the outcomes specified in the principles

[18] Regulation 5 of the NIS Regulations
[19] Regulation 4 of the NIS Regulations
[20] The NCSC security principles can be found here.
[21] The NCSC NIS guidance collection is available here

The Cyber Assessment Framework (CAF)

2.25. This tool provides a systematic method for assessing the extent to which OES are meeting their security duties under the NIS Regulations [22]. It will be used by the Competent Authority when assessing OES or by OES themselves as a self-assessment tool. The CAF provides Indicators of Good Practice against each element of the security principles devised by NCSC providing a structured approach to assess the security and resilience of an OES's network and information systems. The NCSC has developed a collection of supporting guidance intended to assist OES and Competent Authorities in understanding how to meet the cyber security principles of the CAF.

2.26. The CAF is one of the tools used to assess compliance for OES who are in scope of NIS, except for those aspects of OES services which fall within the scope of the requirements laid out in the Smart Energy Code (SEC)[23]. This position may be reviewed in future. OES who are in compliance with the SEC must still comply with other NIS duties other than those in Regulation 10, such as incident reporting duties in Regulation 11.

[22] NCSC Cyber Assessment Framework, available here.
[23] The SEC is a multiparty contract which sets out the terms for the provision of the Data Communications Company's services and specified other provisions to govern the end-to-end management of smart metering in gas and electricity. More information is available here

Chapter 3 – Energy Sector Implementation

Who is in scope?

3.1. There are two ways in which a person can be designated as an OES. Firstly, a person can be deemed to be designated as an OES for an energy subsector under Regulation 8 if they provide an essential service that meets the relevant threshold requirements in Schedule 2 to the NIS Regulations. Secondly, a Competent Authority may designate a person as an OES if the person meets the conditions in Regulation 8(3), even if the person does not meet the threshold requirements.

3.2. Generally, the threshold requirements in Schedule 2 are based on the level of societal or economic impact which could result from disruption to essential services. Persons that meet these thresholds are deemed to be designated as OES and are therefore required to comply with the NIS Regulations. Amendments to the threshold requirements are made from time to time by amending Regulations.

3.3. BEIS recognises that our energy system continues to evolve. There are more distributed and localised energy resources as well as increasing use of smart energy, more flexible energy technologies such as demand side response and storage. The Government is committed to ensuring that good cyber security practices are adopted across the energy sector in Great Britain including for newer technologies. BEIS will be undertaking future work together with Ofgem, HSE and industry to more fully understand how the NIS Regulations may need to be amended to apply to emerging technologies and systems over time.

Roles and Responsibilities

3.4. BEIS is specified in Schedule 1 to the NIS Regulations as the Competent Authority jointly with Ofgem for the electricity subsector[24] and downstream gas with the gas subsector[25]. For the oil subsector and for the upstream gas subsector[26], BEIS is specified as the Competent Authority, but certain compliance and enforcement functions are carried out by HSE under an Agency Agreement[27].

[24] The 'electricity' sub-sector refers to the essential services specified in Schedule 2, paragraph 1 of the NIS Regulations.
[25] '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.
[26] '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.
[27] Agency Agreement between HSE and BEIS available here.

3.5. BEIS is responsible for the overall energy policy framework relating to the NIS Regulations, as well as associated international liaison matters, while the day-to-day compliance and enforcement activities of the Competent Authority are carried out by Ofgem and HSE, with the approach depending on the sub-sector.

3.6. The Competent Authority for each energy subsector is set out in Table 1 below:

Table 1: GB energy sector: Competent Authority roles and responsibilities

Subsector	Competent Authority
Electricity	**Ofgem** (acting jointly with **BEIS**).
Gas	Upstream gas – BEIS with certain compliance and enforcement functions carried out by **HSE** under an Agency Agreement. Downstream gas - Ofgem (acting jointly with **BEIS**).
Oil	**BEIS** with certain compliance and enforcement functions carried out by **HSE** under an Agency Agreement.

3.7. In addition, the Competent Authority functions also include:

- Raising industry awareness of the requirements of the NIS Regulations.
- Ensuring alignment of approaches across the energy sector in Great Britain where appropriate.
- Setting policy on desirable reforms to the requirements of the NIS Regulations and other provisions over time and working with DCMS to amend the Regulations accordingly.
- Keeping pace with the developments within the energy sector in Great Britain.
- Reviewing frameworks of approach to NIS implementation across the energy sector in Great Britain.
- Monitoring the overall cyber security resilience of the energy sector.
- Setting thresholds for OES incident reporting.

3.8. Table 2 below outlines the key responsibilities of BEIS, Ofgem and HSE for the purposes of the NIS Regulations in the energy sector in GB.

Table 2: Overview of the key responsibilities of BEIS, Ofgem and HSE for the purposes of the NIS Regulations in the energy sector in Great Britain:

Function	Body responsible in the gas subsector for downstream gas and the electricity subsector	Body responsible in the oil subsector and the gas subsector for upstream gas
Designation and revocation of OES	BEIS	BEIS
Assessing compliance of OES against the requirements of the NIS Regulations, including using inspections and third-party assessments	Ofgem	HSE
Receipt of incident notification and incident investigations.	Ofgem	HSE
Enforcing compliance with the NIS Regulations.	For matters relating to OES designation, BEIS, otherwise Ofgem	For matters relating to OES designation, BEIS, otherwise, HSE and BEIS
Issuing penalties under the NIS Regulations	For matters relating to OES designation, BEIS, otherwise Ofgem	BEIS

3.9. The duties of Ofgem and HSE in regard to inspections and enforcement are detailed in Chapter 5 below and in their respective NIS industry guidance[28].

Collaboration with Industry

3.10. Outside of the NIS regulatory framework, BEIS collaborates with industry on energy cyber security and wider energy resilience to further national security objectives under the National Cyber Strategy. This work is important in helping to understand, mitigate and respond to cyber threats and to build capacity in the energy sector.

3.11. The BEIS voluntary collaboration and resilience and regulatory energy cyber security policy teams operate separately from each other with split roles and

[28] Links to the relevant Ofgem and HSE guidance documents are available in Annex A

responsibilities. We operate strict information management protocols. Information regarding an organisation's cyber security obtained by the BEIS voluntary collaboration and resilience teams will not normally be shared with the regulatory policy team or used for regulatory purpose unless the organisation has expressly consented. However, subject to any legal constraints on disclosure, BEIS may share information collected as part of the voluntary engagement with a regulator (including Ofgem and HSE) where current practices pose wider issues including but not limited to a possible breach of the NIS Regulations or other relevant regulatory regime; and/or an immediate threat to life, national security, or public safety.

3.12. We operate strict information management protocols. Information regarding an organisation's cyber security obtained by the BEIS voluntary collaboration and resilience teams will not normally be shared with the regulatory policy team or used for regulatory purpose unless the organisation has expressly consented. However, subject to any legal constraints on disclosure, BEIS may share information collected as part of the voluntary engagement with a regulator (including Ofgem and HSE) where current practices pose wider issues including but not limited to a possible breach of the NIS Regulations or other relevant regulatory regime; and/or an immediate threat to life, national security, or public safety.

Information Sharing

3.13. The Competent Authority may share information with other Competent Authorities, relevant law enforcement authorities[29], NCSC as the CSIRT, public authorities in the EU (including the European Commission and the relevant authorities in EU Member States) in accordance with Regulation 6 of the NIS Regulations if that information sharing is necessary for:

- the purposes of the NIS Regulations, or 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 purpose; or
- purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution.

3.14. The information sharing must be limited to information which is relevant and proportionate to the purpose of the information sharing.

3.15. Such information sharing can help to facilitate the sharing of good practice and ensure a consistent implementation approach where appropriate.

3.16. BEIS, Ofgem and HSE work closely with NCSC to ensure that the NCSC produces resources that meet the needs of OES in the energy sector, and to facilitate collaboration on the development of security requirements that reflect

[29] Defined in Regulation 1(2) of the NIS Regulations.

the evolving threats to the sector. As such, BEIS will share information that may be useful in the development of the CAF — such as sharing data on the assessment of operators against the indicators of good practice in the CAF — to ensure that future iterations of the CAF developed by NCSC remain useful and relevant for operators in the energy sector. NCSC may also use this data to develop guidance and technical support that are tailored to the needs of operators in the energy sector.

3.17. The Competent Authorities may also share information in certain circumstances to comply with other legal requirements, for example, under the Freedom of Information Act 2000, the Environmental Information Regulations, or the Data Protection Act 2018.

Chapter 4 – Duties on OES

4.1. This chapter contains a summary of some of the key duties of OES and other parties who may fall within scope of the NIS Regulations.

Designation and Revocation of OES

4.2. In the energy sector, any person (i.e. any legal entity) who provides an essential service of a kind referred to in Schedule 2 will be considered an OES if that service:

a) relies on network and information systems; and

b) satisfies a threshold requirement described for that kind of essential service.

4.3. Organisations that meet the OES threshold under Schedule 2 and rely on network and information systems are deemed to be designated as an OES and are in scope of the NIS Regulations. It is the responsibility of the OES to determine whether they are in scope and to then notify BEIS, in accordance with Regulation 8(2). The notification must be provided within three months after the date on which they meet the requirement to be designated under the NIS Regulations[30].

4.4. If a person is unsure whether they come within the scope of the NIS Regulations, they should contact BEIS to confirm whether they meet the threshold under Schedule 2 of the NIS Regulations[31].

4.5. Any person who thinks they may qualify as an OES under the NIS Regulations should proactively engage with BEIS to seek advice and request resources to assist in their understanding of their designation duties under the NIS Regulations.

4.6. BEIS' overarching approach for implementation is one of collaboration between an OES and the Competent Authority.

Competent Authority Designation Powers

4.7. If BEIS has reason to believe that a person should be an OES, the NIS Regulations contain powers to enable the Competent Authority to obtain the necessary information to determine whether to formally designate that entity

[30] OES who have already notified BEIS of their designation under the NIS Regulations do not need to provide further notification.
[31] OES can contact BEIS via email at nis.energy@beis.gov.uk

as an OES. Chapter 5 sets out the powers available to the Competent Authority.

4.8. The designation power under Regulation 8 may be used in circumstances where an entity does not meet the threshold requirement to be designated as set out above. The Competent Authority may designate that person as an OES for the energy sector if:

a) that person provides an essential service in the energy sector of a kind specified in Schedule 2;

b) the provision of that essential service by that person relies on network and information systems; and

c) the Competent Authority concludes that an incident affecting the provision of that essential service by that person is likely to have significant disruptive effects on the provision of the essential service.[32]

4.9. In order to determine whether to designate such persons as an OES under the NIS Regulations, the Competent Authority will consider[33]:

a) the number of users relying on the service provided by the person;

b) the degree of dependency of the other relevant sectors on the service provided by that person;

c) the likely impact of incidents on the essential service provided by that person, in terms of its degree and duration, on economic and societal activities or public safety;

d) the market share of the essential service provided by that person;

e) the geographical area that may be affected if an incident impacts on the service provided by that person;

f) the importance of the provision of the service by that person for maintaining a sufficient level of that service, taking into account the availability of alternative means of essential service provision;

g) the likely consequences for national security if an incident impacts on the service provided by that person; and

h) any other factor BEIS considers appropriate to have regard to.

4.10. BEIS will notify persons who meet the threshold to be an OES, or who it deems should be an OES under NIS by notice, in writing, served on the person who is to be designated and provide reasons for the designation in the notice. Before exercising the discretionary power to designate under

[32] Regulations 8(3) of the NIS Regulations
[33] Regulations 8(4) of the NIS Regulations

Regulation 8(3), BEIS may invite the person to submit any written representations about the proposed decision to designate it as an OES.

Information required from OES

4.11. An OES designated in scope of the NIS Regulations will be required to provide the following information to BEIS[34]:

a) the registered company name of the OES and the address of the registered UK office

b) the name of any parent entity of the OES, and the registered UK address

c) the name of a NIS Responsible Officer (NRO) along with a Deputy NIS Responsible Officer (Deputy NRO) who can be liaised with in the absence of the NRO

d) contact details for the NRO and Deputy NRO, including their phone numbers, email address, and office address.

4.12. The NRO position is not a regulatory requirement, nor does it require a new or senior appointment. Having a named responsible officer should ensure an OES receives all appropriate NIS related communications from the Competent Authority. BEIS expects this role to also be responsible for notifying the Competent Authority of their status as an OES, and for notification in the event of an incident.

4.13. An OES should maintain effective communication with the Competent Authorities and notify BEIS at the earliest opportunity if they undergo any changes that BEIS should be aware of. For example, where a new NRO is appointed for their organisation.

4.14. An OES should update BEIS in June and December of each calendar year with the NIS NRO's and Deputy NRO's details.

OES established overseas

4.15. An OES is an entity that provides an essential service in Great Britain. This may include an OES who has their head office outside GB. If an essential service relies on networks and information systems that are physically located outside the UK, the relevant OES will still be in scope of the NIS Regulations as long as it provides an essential service in Great Britain.

4.16. An OES which has their head office outside the GB but provides an essential service within GB must nominate in writing, a person in GB to act on their behalf under the NIS Regulations within three months after the date on which

[34] Ofgem guidance available here also sets out information required from OES by Ofgem.

they meet the requirements for designation under the NIS Regulations[35]. The OES must also provide the following information to BEIS:

a) The name and address of the nominated person.

b) Contact details of the nominated person (including an email address and telephone number).

4.17. OES should notify BEIS of any changes to details of the nominated person at the earliest opportunity.

Revocation

4.18. Regulation 9 contains the power for the Competent Authority to revoke a designation of an OES by written notice, if the Competent Authority concludes that an incident affecting the provision of the essential service by an entity would not have significant disruptive effects on the essential service. Before reaching this conclusion, the Competent Authority must also have regard to the factors listed at paragraph 4.10 above.[36]

4.19. If an OES has reasonable grounds to believe that they should no longer be designated as an OES under the NIS Regulations, they must notify BEIS in writing with evidence supporting this belief as soon as practicable.

4.20. The Competent Authority will have regard to such notifications and evidence in considering whether to revoke the OES' designation.

4.21. Before revoking the designation of a person as an OES under Regulation 8, BEIS will:

a) serve a notice in writing of proposed revocation on that person;

b) provide reasons for the proposed decision;

c) invite that person to submit any written representations about the proposed decision within a specified period of time; and

d) consider any representations submitted by the person before a final decision is taken about whether to revoke the designation.

Security duties

4.22. The NIS Regulations require an OES to take appropriate and proportionate:

[35] Regulation 8A of the NIS Regulations.
[36] Regulation 9(4) of the NIS Regulations

- technical and organisational measures to manage the risks posed to the security of the network and information systems on which their essential service relies[37];

- measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services.

4.23. In carrying out their security duties an OES must, having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risk posed.

4.24. The NCSC has defined a set of cyber security principles consisting of 14 top-level principles, with supporting narrative, which are grouped into four high-level objectives[38]. These principles are relevant to all network and information systems supporting the delivery of essential services, including the energy sector. The principles carry no assumptions about how the specified outcomes should be achieved. It is for the OES to determine, working in collaboration with the Competent Authority as necessary, the most appropriate risk-based security measures to deliver these outcomes within their organisational and sectoral contexts.

4.25. It is the Government's view that a risk-based approach, as set out in the security principles, is a more effective way of driving improvements to cyber security in the context of the NIS Regulations than an approach based on prescriptive rules. This is because in complex and rapidly changing areas such as cyber security, prescriptive rules could lead to unintended consequences, misallocation of resources and limited benefits. Organisations should take informed, risk balanced decisions about how they achieve the outcomes specified by the principles, and in turn their security duties as set out in the NIS Regulations and protect the continuity of their essential service against cyber risks.

4.26. It is for an OES to demonstrate compliance with the NIS Regulations by putting in place appropriate and proportionate security arrangements to mitigate any risks posed. Risk management decisions are for an OES to determine based on the activities and operations of their business and taking into account their existing internal management and audit processes, providing that their approach complies with the NIS Regulations. An OES should be able to justify their approach and describe any risk management decisions to their Competent Authority where appropriate.

4.27. To support an OES in meeting the security principles, the NCSC has also published a collection of guidance. Each of the principles is linked to specific guidance which highlights some of the factors that an organisation will usually

[37] Regulation 10(1) of the NIS Regulations.
[38] Available on the NCSC website here

need to consider when deciding how to achieve the outcome and recommends some ways to tackle common cyber security challenges.

4.28. The NCSC's Cyber Assessment Framework (CAF) should be used to assist in determining whether an OES is achieving the outcomes set out in the NCSC security principles unless those services are already covered within the existing compliance scope of the Smart Energy Code (SEC) as previously mentioned. This position may be reviewed in future. An OES who is in compliance with the SEC should be aware that this does not eliminate other NIS duties such as incident reporting.

4.29. The NCSC security principles and the CAF are focused on ensuring baseline cyber security risk management. However, an OES also needs to consider and manage broader resilience risks to the security of their network and information systems. This includes ensuring they are resilient to wider risks such as loss of power supply, hardware or software failure, physical damage, environmental hazards, supply chain risks, development controls and firmware.

4.30. In the upstream gas and oil subsectors, HSE assess compliance with the requirements of the NIS Regulations in the upstream gas and oil subsectors following the principles detailed in the HSE OG86 Operational Guidance, as well as the NCSC CAF.

4.31. An OES is expected to comply with the NCSC CAF security principles when carrying out its security duties under the NIS Regulations. Although the main focus of the NIS Regulations is to respond to the rising cyber security challenge, an OES is expected to identify and manage other security issues in an appropriate and proportionate manner. This includes, for example, physical events that might have an adverse effect on their network and information systems. As such, an OES should also consider broader resilience risks when considering the security of the network and information systems on which their essential service relies such as loss of power supply, hardware or software failure, physical damage, and environmental hazards. Some relevant guidance which an OES may find helpful in relation to broader resilience is provided in Annex A.

Identifying which network and information systems are in scope

4.32. It is a matter for an individual OES to identify which network and information systems are used for the provision of their essential service. The Competent Authority will not specify which network and information systems are in scope, but it may request an OES to share the list of network and information systems which it considers are in scope and the process followed in identifying such systems. The Competent Authority may raise questions about the systems identified, for example should it believe areas, network or information systems are missing that could be critical for the provision of the essential service. NCSC also have guidance that could assist operators to identify critical systems.

Are supply chain or third-party companies in scope?

4.33. Companies in the supply chain of an OES are not deemed in scope of the NIS Regulations as an OES, unless they also satisfy the criteria for designation under Regulation 8. However, in certain circumstances, supply chain or third-party companies who support an OES' provision of their essential service could cause disruption to the provision of the essential service by the OES. As such, the OES should take appropriate and proportionate measures to ensure that these companies have sufficient security standards in place as part of fulfilling their security duties under Regulation 10.

4.34. Competent Authorities may require an OES to provide information relating to their supply chain or third-party operators under Regulation 15(2) and consider this as part of their inspection under Regulation 16. As a matter of good practice, an OES is strongly encouraged to consider the NCSC security principles in their procurement process and use the NCSC guidance to underpin support arrangements with suppliers. NCSC have set out guidance on supply chain related security considerations that should be addressed where relevant to the provision of the essential service.

Incident Notification

4.35. The NIS Regulations mandate the reporting of incidents affecting network and information systems that have a significant impact on the continuity of the essential service which the OES provides[39].

4.36. In Great Britain, a distinction has been made in regard to the incident reporting requirements between:

- reporting for incident management purposes (which, while strongly recommended, will continue to be on a **voluntary** basis); and
- **mandatory** notifications under the NIS Regulations

4.37. This distinction has been made because BEIS would like OES to seek voluntary support from the NCSC and other parts of Government as soon as practically possible after the incident is detected, so that the incident can be contained and further impacts on essential services mitigated. This voluntary collaboration has different objectives to the mandatory reporting requirements specified by the NIS Regulations.

4.38. Details of voluntary incident reporting for cyber non-NIS incidents are set out at Annex E. An OES is encouraged to report all cyber incidents to enable the Government to provide support where required and identify any emerging trends across the sector.

[39] Regulation 11(1) of the NIS Regulations.

NIS reportable incidents

4.39. The requirement to notify incidents under the NIS Regulations relates to any incidents which have a significant impact on the continuity of the essential service which that OES provides (an NIS incident). Incident is defined as any event having an actual adverse effect on the security of network and information systems. In order to determine the significance of the impact of a NIS 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 by the incident.

4.40. In the energy sector in Great Britain, an OES may wish to refer to the sector-specific considerations and thresholds set out in Annex D in determining whether to notify an NIS incident to their Competent Authority. These are provided as guidance only and not exhaustive. The Competent Authority may consider these and other relevant considerations when determining whether an OES' reporting duties under the NIS Regulations have been complied with. The considerations and thresholds set out in Annex C are not intended to override the regulatory provisions and an OES must use its judgment to determine whether an NIS incident should be reported in line with the NIS Regulations.

Process for NIS incident notification

4.41. If an NIS incident occurs, an OES must report this to their relevant Competent Authority. Reports must be made without undue delay and no later than 72 hours after the OES first becomes aware that a NIS reportable incident has occurred[40]. The notification should be in the form of a secure email to the Competent Authority. A template is set out in Annex E (which reflects the information requirements of the Regulations) and contact details can be found in Annex B.

4.42. In the early stages of an incident, much of the detail about the incident may not be known. An OES should complete an initial report to the best of their ability and submit a follow up report as information becomes available. The template in Annex E sets out more detail on the type of information that is helpful in an incident report.

4.43. Operators should ensure that they are following the NIS incident response and recovery guidance as outlined by the NCSC.[41]

Incident response by OES

4.44. It is the responsibility of the OES to manage their incidents and ensure that they receive support if required. The incident response support received

[40] Regulation 11(3)(b)(i) of the NIS Regulations.
[41] The NCSC NIS incident and recovery principles and guidance are available here

under established voluntary frameworks is not a substitute for the OES' incident response processes.

4.45. An OES should have well-defined and tested incident management and mitigation processes in place, that aim to ensure continuity of essential functions in the event of system or service failure and limit the impact of the incident.

4.46. An OES should have incident response plans that:

- are grounded on a comprehensive risk assessment, covering all relevant potential incidents;
- prioritise the systems required to ensure continued effective operations;
- take into account business continuity implications;
- are linked to other business response functions;
- are auditable and testable across a range of incident scenarios (malware infection, insider incident, hacker infiltration, denial of service, etc);
- work seamlessly with other system management and security functions, such as security monitoring; and
- articulate clear governance frameworks and roles with procedures for reporting to relevant internal or external stakeholders, including Ofgem and HSE under the NIS Regulations.

4.47. An OES should regularly assess and test the implementation, effectiveness and efficiency of their incident response plans.

Competent Authority handling of NIS-related incident response

4.48. Following an incident notification, the Competent Authority will assess what further action, if any, is required in respect of that incident. The NIS incident information will also be shared with NCSC as the CSIRT as soon as reasonably practicable.

4.49. Neither BEIS, Ofgem nor HSE are required to provide incident response support. However, if an OES requires incident response support, they should separately report the incident to the NCSC and the BEIS Emergency Response: Capabilities and Operations (ERCO) team as soon as the event is detected. Contact details for the BEIS ERCO team can be found in Annex C

4.50. After receiving an NIS incident notification, HSE or Ofgem may take a number of steps depending on the circumstances of the case, for example:

- check if the OES has been in contact with the NCSC, the ERCO team for incident response support

- for the gas subsector in relation to downstream gas[42] and the electricity subsector[43], check if the OES has been in contact with the BEIS energy resilience team, and Ofgem Incident Response and Governance Group for incident response support in the case on non-cyber incidents;

- monitor the incident as necessary and appropriate;

- liaise with OES for general and resolution support guidance;

- if appropriate, and liaising with BEIS if necessary, depending on the sub-sector, disseminate information for relevant stakeholders, including other OES, about the incident;

- conduct incident investigation and/or NIS inspections if deemed necessary, and

- take enforcement action, if appropriate.

4.51. Following the NIS incident notification, the Competent Authority, or NCSC as the CSIRT, may inform the OES who provided the notification about any relevant information that relates to the NIS incident. This can include any follow up to the incident, in order to assist that OES to deal with the incident more effectively or prevent a future incident. Similarly, they may also inform the public about the NIS incident as soon as reasonably practicable if it is deemed that public awareness is necessary in order to handle that incident or prevent a future incident

4.52. Before the Competent Authority or NCSC informs the public about an NIS incident, the Competent Authority or NCSC will consult each other and the OES who provided the incident notification.

4.53. NCSC, in its capacity as the CSIRT, may inform relevant authorities in other countries under established bilateral information sharing arrangements.

4.54. In addition to the mandatory notification requirements and the voluntary notification mechanisms described in this guidance, the Competent Authority may share information with other Competent Authorities, relevant law enforcement authorities, the CSIRT and the relevant authorities in EU Member States if that information is necessary for:

- the purposes of the NIS Regulations or of facilitating the performance of any functions of a NIS enforcement authority;

[42] '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.
[43] The 'electricity' sub-sector refers to the essential services specified in Schedule 2, paragraph 1 of the NIS Regulations.

- national security purposes; or
- purposes related to the prevention or detection of crime, the investigation of an offence, or the conduct of a prosecution[44]

4.55. Information shared by the Competent Authority must be relevant and proportionate to the purpose of the information sharing[45].

4.56. Ofgem and HSE will maintain logs of all NIS incident reports submitted to them. BEIS will compile an annual report identifying the number and nature of NIS incidents notifications received. The annual report will be shared with NCSC.

Incident investigation

4.57. After an incident notification, the Competent Authority may decide to conduct an investigation, the purpose of which is to:

- assess compliance with the NIS Regulations;
- assess whether the incident was preventable;
- assess whether effective risk management was in place; and
- assess whether the operator had appropriate security measures in place.

4.58. An incident is not in itself a breach of the NIS Regulations and therefore does not automatically mean enforcement action will be taken. If an OES has otherwise complied with their duties under the NIS Regulations and engaged appropriately with Competent Authorities and still suffered an incident, then it is unlikely enforcement action would be taken. Not having reported an incident that meets the incident notification requirements would however be an infringement of the NIS Regulations and may result in enforcement action.

4.59. The Competent Authority may share the results of an incident investigation with the concerned OES, if appropriate. For example, where an OES may find this information useful to improve the resilience of their systems. Ofgem or HSE may provide additional advice tailored to the relevant OES in relation to incident preparedness.

[44] Regulation 6(1)(a) of the NIS Regulations
[45] Regulation 6(1)(b) of the NIS Regulations

Chapter 5 – Competent Authority Approach to Enforcement, Compliance and Penalties

5.1. Oversight and enforcement of the NIS Regulations is the responsibility of the designated Competent Authority. Chapter 3 above details the relevant roles and responsibilities for each organisation in regard to enforcement.

Information requests by the Competent Authority

5.2. The Competent Authority is able to request information from OES under Regulation 15.

5.3. In order to assess whether a person meets the Schedule 2 threshold requirements to be deemed to be designated as an OES or meets the conditions in Regulation 8(3) to be designated by the Competent Authority, the Competent Authority may serve an Information Notice on a person[46].

5.4. An Information Notice can also be served on an OES requiring it to provide the Competent Authority with all such information as it reasonably requires for one or more of the following purposes[47]:

a) to assess the security of the OES's network and information systems;

b) to establish whether there have been any events that the Competent Authority has reasonable grounds to believe have had, or could have, an adverse effect on the security of an OES's network and information systems and the nature and impact of those events;

c) to identify any failure of an OES to comply with any duty set out in the NIS Regulations;

d) to assess the implementation of the OES's security policies, including from the results of any inspections conducted under Regulation 16, and any underlying evidence in relation to such an inspection.

5.5. Where an Information Notice is served, the Notice must:

a) describe the information that is required;

b) provide the reasons for requesting such information;

[46] Regulation 15(1) of the NIS Regulations
[47] Regulation 15(2) of the NIS Regulations

c) specify the form and manner in which the requested information is to be provided; and

d) specify the time period within which the information must be provided.

5.6. An Information Notice may be served on an OES, or where the Competent Authority does not have specific contact details (such as where the Information Notice is served to establish whether a person should be designated as an OES), the Notice may be served in a manner that the Competent Authority considers appropriate to bring it to the attention of the relevant person(s). The Information Notice may also take the form of a general request for a certain category of persons to provide the information specified in the notice[48].

5.7. OES must comply with the requirements of an Information Notice[49]. A failure to comply may lead to enforcement action. Further information on the different types of enforcement action can be found below in this chapter.

Power of Inspection

5.8. The Competent Authority may conduct inspections (or appoint, or direct the appointment of, a person to conduct inspections on its behalf) in accordance with Regulation 16 of the NIS Regulations.

5.9. Inspections will be used for the purpose of:

- verifying compliance with the requirements of the NIS Regulations;
- assessing or gathering evidence of potential or alleged failures to comply with the requirements of the NIS Regulations; or
- any follow-up activity for the above purposes[50].

5.10. OES have a number of duties in relation to inspections. These include co-operating with the inspector and providing reasonable access to their premises. OES must also allow the inspector to examine, copy or remove such documents or information as the inspector considers relevant. This may include information held electronically. The OES must allow the inspector access to any party from whom the inspector seeks relevant information for the purposes of the inspection.

5.11. An inspector may, among other powers the inspector may exercise under Regulation 16:

- take a statement or statement from any individuals;

[48] In accordance with Regulations 15(6) and applies to Notices served under Regulations 15(1) only.
[49] Regulation 15(5A) of the NIS Regulations.
[50] Regulation 16(9) of the NIS Regulations.

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

5.12. For the purpose of carrying out any inspection, the OES must comply with any requests made by, or requirement of, an inspector performing their functions under the NIS Regulations and pay the reasonable costs for an inspection if so required by the Competent Authority. The processes and regimes to recoup reasonable costs will be set out in greater detail in Ofgem and HSE's guidance.

5.13. If directed by the Competent Authority, an OES must appoint a person approved by the Competent Authority to conduct an inspection on the Competent Authority's behalf under Regulation 16(1)(c) of the NIS Regulations.

5.14. In the oil and upstream gas subsectors, HSE conduct inspections on the basis of their OG86[51] operational guidance which sets out the security profiles that OES in that subsector are expected to meet.

5.15. An inspection may cover several areas including but not limited to, the assessment of the improvement plans against the current security profile in their relevant subsector. Inspectors have the power to take any action that they consider appropriate and reasonably required for the purpose of the inspection including[52]:

- entering an OES's premises (except any premises used wholly or mainly as a private dwelling) at any reasonable time if the inspector has reasonable grounds to believe entry may be necessary or helpful for the purpose of carrying out an inspection;
- requiring the 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 to the inspection;
- requiring the 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;
- examining, printing, copying or removing any document or information, and examining or removing 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 to the inspection;

[51] HSE Operational Guidance OG86, available here.
[52] Regulation 16(5) of the NIS Regulations

- taking a statement or statements from any person; and
- conducting, or directing the OES to conduct, tests.

5.16. When exercising the inspection powers, the Competent Authority and their inspectors will show proof of identification if so requested by the relevant OES.

5.17. The Competent Authorities in the energy sector will generally seek to make arrangements for inspections through agreement with the relevant OES, where this is appropriate. If the Competent Authority exercises its powers of entry under the NIS Regulations, inspectors will have regard to the Code of Practice on Powers of Entry when exercising any function to which the Code relates[53].

Enforcement Regime

5.18. Where appropriate, the Competent Authority may issue an Enforcement Notice or Penalty Notice.

5.19. Information in this section relates to enforcement activity handled by BEIS: namely enforcement for designation matters in the energy sector, and enforcement in the upstream oil and gas subsectors. Ofgem is responsible for all other enforcement issues not related to designation matters in the gas subsector[54] in relation to downstream gas and electricity subsector. References to "the Competent Authority" in this section therefore relates to BEIS in relation to designation matters or HSE acting on behalf of BEIS in relation to enforcement in the upstream oil and gas subsectors.

Enforcement Notice

5.20. The Competent Authority may serve an Enforcement Notice if it has reasonable grounds to believe the OES has failed to comply with one or more of the duties specified in Regulation 17(1) of the NIS Regulations.

5.21. The Competent Authority may serve more than one Enforcement Notice if the Competent Authority considers that the OES has committed more than one breach, and one Enforcement Notice can also be used to cover multiple breaches. The scope of any enforcement action may also widen if the Competent Authority becomes aware of other potential contraventions.

[53] Powers of Entry: Code of Practice, available here.
[54] '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.

5.22. Before serving an Enforcement Notice, the Competent Authority will inform the OES in a form and manner that the Competent Authority considers appropriate having regard to the facts and circumstances of the case[55] of:

a) the alleged failure; and

b) how and when representations may be made in relation to the alleged failure and any related matters.

5.23. When the Competent Authority so informs the OES, it may also provide the OES with notice of its intention to serve an Enforcement Notice.

5.24. The OES should submit any evidence it wishes to put forward to support its representations.

5.25. The Competent Authority may serve an Enforcement Notice on an OES within a reasonable time after the OES has been informed as set out at paragraph [5.23] above having regard to the facts and circumstances of the case, irrespective of whether it has provided any notice to the OES of its intention to serve such a Notice.

5.26. An Enforcement Notice must be in writing and must specify:

a) the reasons for serving the notice

b) the alleged failure which is the subject of the notice, and

c) what steps, if any, must be taken to rectify the alleged failure and the time period within which such steps must be taken.

5.27. An OES served with an Enforcement Notice must comply with the requirements, if any, of the notice regardless of whether they have paid any penalty imposed under the NIS Regulations.

5.28. If, having considered any representations made by the OES, or any steps taken by the OES to rectify the alleged failure, the Competent Authority is satisfied that no further action is required, the Competent Authority will inform relevant OES of this in writing as soon as reasonably practicable.

5.29. Should the relevant OES wish to be provided with the reasons why the decision to take no further action was taken, they can request these within 28 days of being informed of that decision. Upon receiving such a request, the Competent Authority must provide written reasons within a reasonable time and no later than 28 days after receipt of the request.

[55] Regulation 17(2A) of the NIS Regulations.

Penalty Notices

5.30. In the energy sector in GB, BEIS is responsible for issuing penalties for contraventions of an OES's NIS duties in relation to designation matters for all energy subsectors, as well as all penalties for the oil[56] and upstream gas[57] subsectors. Ofgem is responsible for all other penalties in the gas subsector in relation to downstream gas[58] and the electricity[59] subsector.

5.31. The primary objective in issuing a Penalty Notice under the NIS Regulations is to promote high behavioural standards amongst OES and to ensure compliance with the NIS Regulations. The aim of serving a Penalty Notice is to address the contraventions or failure to comply with the NIS Regulations and thereby deter OES from committing further contraventions or failures in future.

Notice of intention to issue a Penalty Notice

5.32. The Competent Authority may serve a notice of intention to impose a penalty on an OES if it has reasonable grounds to believe that the OES has failed to comply with a duty referred to in Regulation 17(1) or the duty set out in Regulation 17(3A) and considers that a penalty is warranted having regard to the facts and circumstances of the case.

5.33. The notice of intention to impose a penalty must be in writing and specify the information set out in Regulation 18(3). That is, the notice must specify the reasons for imposing a penalty, the sum that is intended to be imposed as a penalty and how it 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 served, 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.

5.34. In response to such notice, an OES may submit representations (including supporting evidence) and must do so within the deadline stipulated in the notice of intention to impose a penalty. Any representations submitted after that deadline may not be considered.

5.35. The Competent Authority may issue a notice of intention to impose a penalty in respect of multiple contraventions, and it may serve a notice of intention to

[56] The threshold requirements for essential services in the 'oil subsector' are specified in Schedule 2, paragraph 2 of the NIS Regulations.
[57] '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.
[58] '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.
[59] The 'electricity' sub-sector refers to the essential services specified in Schedule 2, paragraph 1 of the NIS Regulations.

impose or impose a Penalty Notice regardless of whether it is serving or has served an Enforcement Notice on an OES.

Issuing a Penalty Notice

5.36. After considering any representations submitted by the relevant OES in accordance with the requirements in the notice of intention, the Competent Authority may serve a Penalty Notice with a final penalty decision on the OES if the Competent Authority is satisfied that a penalty is warranted having regard to the facts and circumstances of the case.

5.37. The sum imposed by a Penalty Notice may be that indicated in the notice of intention, or such a penalty as the Competent Authority considers appropriate and proportionate to the failure in respect of which it is imposed

5.38. The Competent Authority will inform the OES in writing if it decides against issuing a penalty after considering the circumstances of the case and any representations made by the OES.

5.39. A Penalty Notice must be given in writing and must:

a) include the reasons for the final penalty decision;

b) require the OES to pay:

   a. the penalty specified in the notice of intention to impose a penalty; or

   b. such penalty as the Competent Authority considers appropriate in light of any representations made by the OES and any steps taken by the OES to rectify the failure or to do one or more of the things required by an Enforcement Notice;

c) the period within which the penalty must be paid (“the payment period”) and the date on which the payment period is to commence;

d) details of the appeal process to the First-tier Tribunal; and

e) the consequences of failing to make payment within the payment period.

5.40. It is the duty of the OES to comply with the requirements imposed by a Penalty Notice.

Determining the penalty amount

5.41. The amount that can be imposed on an OES is subject to the maximum amounts for various penalty categories specified in Regulation 18(6) of the NIS Regulations.

5.42. The Competent Authority must determine a sum that is appropriate and proportionate to the failure in respect of which it is imposed, and which is within the relevant penalty category in Regulation 18(6).

5.43. Where the Competent Authority decides that it is appropriate to serve a Penalty Notice, the following steps will be taken to determine the appropriate sum to be imposed as the penalty:

- assess the contravention or failure and identify the applicable penalty category;
- assess the seriousness of the contravention or failure and place within the applicable identified penalty category;
- consider aggravating and mitigating factors;
- consider an adjustment for deterrence; and
- establish the total financial liability.

5.44. These steps are considered in further detail below:

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

5.45. Regulation 18(6) sets out three capped penalty categories. Accordingly, the first step the Competent Authority will take in determining the sum of any penalty is to identify the category that best reflects the nature of the contravention or failure. The NIS Regulations identify categories with an upper cap, however no minimum amounts are identified. For example, a penalty must not exceed £1,000,000 for any contravention which the Competent Authority determines is not a material contravention. Thus, the penalty for such a contravention can be any amount up to £1,000,000.

5.46. In identifying the applicable penalty category for any contravention or failure, the Competent Authority will apply the following criteria in accordance with the NIS Regulations:

- a category one penalty will be identified for any contravention or failure which the Competent Authority determines was not a material contravention. Such penalties will not exceed £1,000,000;
- a category two penalty will be identified for any material contravention which the Competent Authority determines does not meet the criteria set out for a category three penalty. A category two penalty will not exceed £8,500,000;
- a category three penalty will be identified for any material contravention which the Competent Authority determines 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.

5.47. In practice this step will firstly involve determining whether the contravention or failure was a material contravention. Any contravention or failure which is not material will fall into category one set out above.

5.48. A material contravention[60] is defined for the purposes of the NIS Regulations as 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 to comply with one or more of the duties under Regulations 17(1)(a) to (d) or 17(2)(a) to (d). Where an Enforcement Notice was not served or no steps were required to be taken pursuant to an Enforcement Notice, a material contravention refers to a failure to comply with one or more of the duties under Regulations 17(1)(a) to (d) or 17(2)(a) to (d).

5.49. 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); and
- failure to notify an incident as required by regulation 12(9);

5.50. Failures which are not treated as a material contravention will therefore generally include those relating to:

- failure to notify the Competent Authority under Regulations 8(2);
- failure to comply with the requirements stipulated in Regulations 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.

<u>Step 2: Assess the contravention or failure within the identified penalty category</u>:

[60] As defined under Regulations 18(7)(a) of the NIS Regulations

5.51. The Competent Authority will next identify an amount which reflects the contravention or failure within the applicable 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. The factors that will be considered 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

Step 3: Consider aggravating and mitigating factors:

5.52. When the applicable penalty category, and the appropriate penalty level within the category has been identified, the Competent Authority will consider an adjustment to reflect any relevant aggravating or mitigating factors. These factors generally relate to matters including (without limitation) the OES' compliance history, and the OES' actions (or lack thereof) after it becomes aware of the contravention or failure, whether before or after the Competent Authority opens any enforcement case. Examples of aggravating factors which would tend to increase the penalty amount include, but are not limited to:

- continuation of the contravention or failure after becoming 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 attempts to conceal all or part of a contravention or failure from the Competent Authority;

- failure to cooperate fully with reasonable requests from the Competent Authority's investigating team; and

- whether the contravention or failure was a repeat of a previous contravention or failure or part of a pattern of non-compliance.

5.53. Examples of mitigating factors which would may decrease the penalty amount include, but are not limited to:

- 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 that do not constitute a NIS incident to the Competent Authority;

- appropriate action by the OES to remedy the contravention after becoming aware of it;

- evidence that the OES has taken steps to review its compliance activities and change them as appropriate in light of the events that led to the investigation at hand; and

- cooperating with the Competent Authority'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.

5.54. The lists of aggravating and mitigating factors are not exhaustive. The factors will be applied on a case-by-case basis and may not all be applied to a particular contravention by an OES. The Competent Authority will decide the relevant aggravating and mitigating factors depending on the circumstances of each case.

5.55. OES should promptly self-report potential contraventions. For example, if an OES carries out internal checks and realises that they have misreported information to the Competent Authority then they should promptly provide corrected information to the Competent Authority. Prompt, accurate and comprehensive self-reporting will count in an OES's favour, particularly when those breaches were unlikely to come to light via other information sources.

<u>Step 4: Consider an adjustment for deterrence</u>:

5.56. The Competent Authority will next consider whether a further adjustment to the penalty is required within the applicable penalty category to help ensure the penalty will have a sufficient deterrent effect. Such an adjustment may be

made if the Competent Authority considers 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:

5.57. Having carried out the steps above, the Competent Authority will consider the total 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. The Competent Authority may at this stage consider the effect of a proposed penalty on the financial viability of an OES and may make adjustments accordingly.

5.58. Any upwards adjustments considered under steps 3, 4 or 5 are subject to the maximum penalty amounts for a contravention or failure set out in Regulation 6 and at Step 1 above.

Other Relevant Information

5.59. A Penalty Notice will specify a payment period by which the penalty must be made. OES must comply with any requirements imposed by a Penalty Notice and penalties must be paid before the end of the payment period which begins on the date that the Penalty Notice is served. Failure to comply with the payment may result in the Competent Authority taking steps to recover the outstanding sum such as registering the outstanding sum as a civil debt.

5.60. An OES may appeal against a penalty decision made in relation to that OES. Please refer to Chapter 6 of this guidance for details of the appeal process.

General Enforcement Considerations

5.61. Before the Competent Authority takes any enforcement action under the NIS Regulations, the Competent Authority must consider whether it is reasonable and proportionate to act in relation to the contravention based on the facts and circumstances of the case[61].

5.62. The Competent Authority must have regard to the following:

- any representations made by the OES about the contravention and the reasons for it, if any;
- any steps taken by the OES to comply with the requirements of the NIS Regulations;
- any steps taken by the OES to rectify the contravention;

[61] Regulation 23 of the NIS Regulations.

- 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 enactment.

Disclosure of Notices

5.63. The Government is committed to being transparent and fair throughout the enforcement process and, where possible, visible in the actions we take. Publishing notices can encourage accountability and drive compliance with the NIS requirements.

5.64. Where an Enforcement Notice and/or Penalty Notice has been served on an OES, the Competent Authority may decide to publish the notice in full or in redacted form or publish limited information. The Competent Authority will consider what information, if any, to publish on a case-by-case basis.

5.65. While aiming to be as transparent as possible, the Competent Authority will also give due regard to concerns around confidentiality, any potential impact on the ability to investigate as well as other relevant considerations, for example any security concerns. The Competent Authority will always seek to ensure OES are treated fairly and appropriately.

Civil Proceedings

5.66. If the Competent Authority has reasonable grounds to believe that an OES has failed to comply with the requirements of an Enforcement Notice within the timeframe stipulated in the notice, the Competent Authority may commence proceedings against the OES for:

- an injunction to enforce the duty to comply with the requirements of an Enforcement Notice in Regulation 17(3A);
- specific performance of a statutory duty under section 45 of the Court of Session Act 1998; or;
- for any other appropriate remedy or relief[62].

5.67. Civil proceedings must be brought before a civil court in the UK no sooner than 28 days after the day the last relevant Enforcement Notice was served on the OES[63].

5.68. Civil proceedings may be commenced irrespective of whether an OES has appealed to the First-tier Tribunal...

[62] Regulation A20 of the NIS Regulations.
[63] Regulation 20A(1)(a) of the NIS Regulations.

5.69. The Government will take a proportionate approach in determining whether civil proceedings are appropriate before civil proceedings are issued. However, it may be necessary to act through the Courts to enforce compliance if an OES does not take steps to comply with an Enforcement Notice.

5.70. Where possible, the OES will be notified prior to the commencement of civil proceedings, unless the Competent Authority determines that such action must be taken without delay, for example, where the failure to take steps to comply with an Enforcement Notice could cause significant risks to a third parties including service users or members of the public.

Whistleblowing

5.71. 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. Parties who may have such information relating to the energy sector are invited to contact the Competent Authority. Disclosures made to "blow the whistle" about concerns regarding potential breaches of relevant regulations or legislation may lead to enforcement and/or compliance action.

5.72. To facilitate such disclosures, the Government has issued whistleblowing guidance[64] 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.

Informal Resolution

5.73. In certain circumstances, the Competent Authority may seek an informal resolution to bring an OES into compliance and remedy the consequences of any contravention or failure. This can be done before or during the formal enforcement process or alongside it.

5.74. In many circumstances seeking an informal resolution will not be appropriate when addressing potential breaches of the NIS Regulations. However, there are many circumstances in which it can lead to an effective outcome.

5.75. The Competent Authority may pursue one or more of the following actions as part of the informal resolution with the relevant OES:

[64] Whistleblowing Guidance and Code of Practice, available here.

- agree with the OES 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 failure;

- 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 Competent Authority recommendations;

- agree with the OES that the OES should 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 the persons' recommendations;

- accept agreed voluntary undertaking or assurances by the OES to ensure future compliance; or

- the OES agree to other voluntary action, such as implementing specified remedial or improvement actions.

5.76. If the Competent Authority decides that an informal resolution is suitable for resolving an issue, the Competent Authority will need to be satisfied that the action will fully address the relevant concerns. In making this decision, the Competent Authority will have regard to whether:

- where issues have been self-reported (and are not NIS incidents as defined in Regulations 11 of the NIS Regulations), the Competent Authority is 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 through other means, the Competent Authority is satisfied that the full extent of the potential contravention or failure has been established;

- where applicable, the Competent Authority is satisfied that the OES has fully complied with the duty to notify NIS incidents in Regulation 11;

- the Competent Authority is 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 action and will be implemented effectively

5.77. OES are expected to engage fully and proactively in helping to ensure a successful informal resolution. If the Competent Authority is not satisfied with

an OES's engagement, they 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, the Competent Authority will take seriously any evidence that an OES has reneged on assurances, voluntary undertakings or other agreements that form part of an informal resolution.

5.78. When an informal resolution has been successful, the matter will normally be closed. However, one outcome could be a period of compliance monitoring after closure.

Chapter 6 – Appeals

6.1. In accordance with Regulation 19A, an OES may appeal to the First-tier Tribunal against one or more of the following decisions of the Competent Authority to:

a) designate that person as an OES

b) revoke the designation of that OES

c) serve an Enforcement Notice on that OES,

d) serve a Penalty Notice on that OES.

6.2. The OES may appeal on one or more of the following grounds ("the grounds of appeal"):

a) that the decision was based on a material error as to the facts

b) that any of the procedural requirements under the NIS Regulations in relation to the decision have not been complied with and the interests of the OES have been substantially prejudiced by the non-compliance

c) that the decision was wrong in law

d) that there was some other material irrationality, including unreasonableness or lack of proportionality which has substantially prejudiced the interests of the OES.

6.3. OES may submit a notice of appeal[65] within 28 days of the date on which the relevant decision or Notice was received. If an OES misses the 28-day deadline, they may submit reasoning for missing the deadline to the Tribunal. The Tribunal will make the final decision to hear such an appeal after considering the information provided by the OES.

6.4. The First-tier Tribunal will determine the appeal in accordance with Regulation 19B, taking into account the grounds of appeal and by applying the same principles as would be applied by a court on an application for judicial review.

6.5. The First-tier Tribunal may, until it has determined the appeal, and unless the appeal is withdrawn, suspend the effects of the whole or part of any of the decision which the OES is appealing. If an Enforcement Notice is not suspended in whole or part by the First-tier Tribunal, then it (or relevant parts of it) remain in force and can be enforced.

6.6. After considering the OES's appeal, the First-tier Tribunal may confirm any decision to which the appeal relates or quash the whole or part of a decision to which the appeal relates. Where the Tribunal quashes the whole or part of a decision, it will remit the matter back to the Competent Authority with a

[65] Form T98: Notice of appeal, available here.

direction to reconsider the matter and make a new decision having regard to the ruling of the First-tier Tribunal.

6.7. The Competent Authority will reconsider the matter having regard to the direction of the First-tier Tribunal. If the Competent Authority makes a new decision, this will be considered final.

6.8. The appeal process is governed by the General Regulatory Chamber tribunal procedure rules ("the GRC rules")[66]. The GRC rules set out the procedural rules for proceedings before the First-tier Tribunal, including by when and how an OES should appeal and how hearings are conducted.

[66] General Regulatory Chamber tribunal procedure rules, available here.

Chapter 7 – National and International Co-Operation

National

7.1. There are multiple Competent Authorities in the UK which regulate the OES and relevant digital service providers (RDSPs) in the sectors covered by the NIS Regulations. DCMS is responsible for the overall NIS Regulations Framework and BEIS works closely with them in continuing to develop the regulatory framework to ensure it remains fit for purpose. BEIS will work with other Competent Authorities and the Devolved Administrations to develop shared capability and support structures, in order to ensure that the NIS Regulations are applied in a consistent, coherent and equitable manner across the sectors in the UK. This is especially important where there are operators that provide essential services in more than one sector, and therefore fall within the remit of more than one Competent Authority.

International

7.2. The NCSC in its role as the SPOC is responsible for cross-border liaisons, facilitating cooperation and communication where possible. The NCSC compiles annual reports from the Competent Authorities containing the number of incidents and the nature of these incidents. Competent Authorities are required to provide this information on an annual basis.

Annex A – Broader Regulatory Guidance

7.3. The following resources are existing guidance related to network and information systems in the energy sector which OES may find helpful.

Table 3: Broader Energy Sector Regulatory Resources

Standard or guidance	Description
Ofgem NIS Guidance for the downstream gas and electricity subsectors	Guidance for OES in the gas subsector in relation to downstream gas and the electricity subsector setting out how Ofgem will carry out its regulatory functions under the NIS Regulations
Ofgem Enforcement Guidance https://www.ofgem.gov.uk/publications-and-updates/enforcement-guidelines	Guidelines on Ofgem's enforcement policies and processes which sets out the alternatives tools that Ofgem might use to exercise the relevant enforcement powers under NIS.
Relevant HSE Enforcement Guidance **Enforcement policy statement:** https://www.hse.gov.uk/enforce/enforcepolicy.htm **Regulation of Health and Safety at work HSE51:** Available here **How HSE Regulates:** https://www.hse.gov.uk/enforce/index.htm	Guidance utlisied by HSE inspectors in conducting inspections and taking enforcement action.

Annex B – Broader resilience of networks and information systems

7.4. The following resources are examples of existing guidance and standards that include elements related to broader resilience risks to network and information systems which OES may find helpful.

Table 4: Broader Cyber Resilience Resources

Standard or guidance	Description
The Centre for Protection and National Infrastructure (CPNI) Website https://www.cpni.gov.uk/advice-guidance	A useful resource for all organisations is te CPNI website which contains advice and guidance on many aspects of physical and personnel security.
ISO27001 https://www.iso.org/standard/54534.html	This standard specifies the requirements for establishing, implementing, and maintaining an information security management system. Section A.11 covers physical and environmental security.
NIST cyber security framework https://www.nist.gov/cyberframework	This framework was developed by the US Government in collaboration with the private sector and contains a set of industry standards and best practice to support organisations in managing cyber risks. The framework is a set of cyber security activities, outcomes, and informative references that are common across critical infrastructure sectors. The following elements of the framework core provide some useful guidance and further references: • PR.AC-2 – Physical access to assets is managed and protected • PR.AT-5 – Physical and information security personnel understand roles and responsibilities • PR.IP-5 – Policy and regulations regarding the physical operating environment for organisational assets are met, and

	• DE.CM-2 – The physical environment is monitored to detect potential cyber security events.
IEC-62443	IEC-62443 is a series of standards including technical reports to secure Industrial Automation and Control Systems (IACS). It provides a systematic and practical approach to cybersecurity for industrial systems. Every stage and aspect of industrial cybersecurity is covered, from risk assessment through operations. Refer to IEC62443 Part 2-1/ Page 27: table 9- Physical and environmental security: requirements.
Cloud Control Matrix https://downloads.cloudsecurityalliance.org/initiatives/ccm/CSA_CCM_v3.0.xlsx	The Cloud Controls Matrix is a cybersecurity control framework for cloud computing produced by the Cloud Security Alliance (CSA). Its control objectives cover some useful business continuity measures: • BCR-03 - Data centre utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions; • BCR-05 - Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied; • BCR-06 - To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance

Annex C – Contacts

Table 4: Relevant contacts

Body	Contact
BEIS Regulatory Policy team	Generic: nis.energy@beis.gov.uk NIS incident notification: erco@beis.gov.uk
Ofgem	Generic: cybersecurityteam@ofgem.gov.uk NIS incident notification: cyberincident@ofgem.gov.uk
HSE	NIS.Cyber.Incident@hse.gov.uk
NCSC	Email - incidents@ncsc.gov.uk Telephone (24/7) – 0300 020 0973
DCMS	NIS policy team: nis@dcms.gov.uk

Annex D – Incident Reporting Thresholds

7.5. BEIS have worked with Ofgem and HSE to determine the arrangements for incident reporting for the downstream gas[67] services within the gas subsector and electricity[68] subsector in the GB energy sector.

7.6. These thresholds set out below are for guidance only and as referred to at paragraph 4.41 in this guidance, there may be circumstances outside of these which need to be reported. We will be monitoring the application of the thresholds over time and through discussions with industry to ensure that they remain fit for purpose.

Table 5: NIS Incident Reporting Thresholds for Downstream Gas Subsector and Electricity Subsector

Essential service[69]	Incident thresholds
Gas Transmission	Loss of supply or outage that has or is likely to lead to loss of supply to offtakes and affects customers.
Electricity Transmission	Loss of supply or outage that has or is likely to lead to loss of supply to grid supply points and affects customers for more than 3 minutes
Gas Distribution	Unplanned single incident loss of supply to 5,000 customers.
Electricity Distribution	Unplanned single incident loss of supply to 50,000 customers for more than 3 minutes.
Gas Interconnectors	Unplanned loss of ≥10MCM over a 24-hour period.
Electricity Interconnectors	The net unauthorised or unplanned loss or gain of ≥560MW of interconnector flow in a given direction.
Electricity Generation	The unauthorised or unplanned loss of ≥1500MW of electricity generation, when cumulated with all generators operated by

[67] '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.
[68] The 'electricity' sub-sector refers to the essential services specified in Schedule 2, paragraph 1 of the NIS Regulations.
[69] Refer to the relevant definitions in Schedule 2, paragraphs 1 and 3 of the NIS Regulations.

	affiliated undertakings[70]. This includes generation scheduled to dispatch within the next 4 hours.
Electricity Suppliers	Unplanned shut off or single incident loss of supply to 50,000 customers for more than 3 minutes.

Table 6: NIS Incident Reporting Thresholds for Oil Subsector

Essential service[71]	Incident thresholds
Oil transmission by pipeline	Loss of >[20]% of supply for >24 hours
Operators of oil production, refining and treatment facilities, storage and transmission	Loss of >[20]% of supply for >24 hours
Conveyance of oil through a relevant upstream petroleum pipeline	Unplanned loss of conveyance > 8,219 tonnes oil equivalent over 24-hour period
Operation of relevant oil processing facilities	Unplanned loss of conveyance > 8,219 tonnes oil equivalent over 24-hour period
Operation of petroleum production projects other than a project which is primarily used for the storage of gas	Unplanned loss of conveyance > 8,219 tonnes oil equivalent over 24-hour period
Operation of gas storage facilities	Unplanned loss of >10MCM (or 8,219 tonnes oil equivalent) over 24-hour period
Operation of LNG facilities	Unplanned loss of >10MCM (or 8,219 tonnes oil equivalent) over 24-hour period
Operation of gas processing facilities	Unplanned loss of conveyance > 8,219 tonnes oil equivalent over 24-hour period

[70] "Affiliated undertakings" are defined in the NIS Regulations, Schedule 2, paragraph 1(8)(a).
[71] Refer to the relevant definitions in Schedule 2, paragraph 2 of the NIS Regulations.

Annex E – Incident Reporting Template

This form should be used by OES to capture information on NIS incidents which must be sent to Ofgem or HSE.

For Ofgem: cyberincident@ofgem.gov.uk

For HSE: NIS.Cyber.Incident@hse.gov.uk

Mandatory reporting: An OES is under a duty under Regulation 11 of the NIS Regulations to notify the Competent Authority about any incident which has a significant impact on the continuity of the essential service that the OES provides. Reports must be made as soon **as possible and no later than 72 hours after the OES is aware that a reportable incident has occurred**.

Voluntary reporting: This form can also be used by OES to report other cyber incidents to BEIS and the NCSC on a voluntary basis. For more information on voluntary cyber incident reporting, see Annex E.

Due to the sensitivity of the information included in the incident notification, **OES must submit the incident notifications through encrypted email**. Switch Egress, is currently certified under the NCSC Commercial Product Assurance scheme and is also deemed appropriate for use. OES may use other secure systems that they operate.

Points to capture	Response
Contact information • Name of the person submitting the notification. • Role in the company • Phone number • Email address	
Organisational details • Name of the Organisation and the essential service it provides. • Sites/assets affected • Internal incident ID number or name.	
The Incident • Date and time incident detected	

Points to capture	Response
• Date and time incident occurred • Date and time incident reported	
Type of incident Cyber / non-cyber / both	
Incident status Detected incident / suspected incident	
Incident stage Ongoing / ended / ongoing but managed	
Cyber incidents – Please provide a summary of your understanding of the incident, including any impact to services and/or users, including: • Incident type(s) • Description of the incident(s) • How the incident was discovered • Duration of the incident(s) • Location(s) of the incident(s) • Services/systems affected • Impact on those services/systems • Impact on safety to staff or public • Suspected cause • Whether there is any known or likely cross-border impact • Any other relevant information	
Root cause of incident System failure/natural phenomena/human error/malicious actions/third party failures/ other (if other, please explain)	
Categorisation of the incident (e.g.) intrusion, denial of service etc.	
Severity of the threat: major/high/medium/low	
Other relevant information	
Mitigations What investigations and/or mitigations have you or a third party performed or plan to perform.	
Who else has been informed about this incident?	

Points to capture	Response
(CSIRT, NCSC, NCA, other Member States etc.)	

To request a Word copy of this template please email: nis.energy@beis.gov.uk

Annex F – Voluntary Incident Reporting Guidance and Contacting BEIS and NCSC

Voluntary incident reporting to NCSC

BEIS undertakes voluntary collaboration work on energy cyber security, in partnership with NCSC and, to further national security objectives. This is important work and valuable to all parties, so we wish it to continue to help us understand, mitigate, build capability, and respond to cyber threats to the energy sector.

BEIS has produced the following cyber incident reporting guidance in collaboration with the NCSC to provide instructions for the OES and other designated by the Government as Critical National Infrastructure (CNI)[72] operators regarding the reporting of cyber incidents.

You are encouraged to notify the NCSC when you are facing a cyber incident which

a) You require NCSC's support to manage (in communications this should be marked '**REQUEST ASSISTANCE**'

OR

b) You consider is of wider interest (in communications this should be marked '**FOR INFORMATION ONLY**')

'**REQUEST ASSISTANCE**: The NCSC will provide advice, guidance and, where resources allow, support for cyber incidents that:

- Disrupt UK essential services or CNI (including any that meet or are likely to meet NIS reporting thresholds); or
- Result in a significant loss of data important to the ongoing operation of your organisation, including loss of sensitive information or intellectual property; or
- Indicate unauthorised access or malicious software on key IT systems which you are unable to resolve yourselves.

[72] CNI are national assets that are essential for the functioning of society. More information on CNI is available on the Centre for Protection of National Infrastructure website, here.

'**FOR INFORMATION ONLY**': The NCSC is keen to receive notification of incidents that OES (or wider CNI organisations) assess are noteworthy, either at the time or post-investigation. This includes incidents that could:

- Add to our understanding of adversary activity
- Inform the advice and guidance that we provide
- Help to protect other organisations.

When contacting the NCSC:

- The NCSC's Incident Management team are contactable on a 24/7 basis though this webform.
- Please put in the header of any messages to NCSC whether your message is '**REQUEST ASSISTANCE**' or '**FOR INFORMATION ONLY**'. This will assist with triage and, when appropriate, help to expedite support from the NCSC.
- Recognising resource constraints, you may only receive an automated response to 'FOR INFORMATION' submissions, but your information will be gratefully received and analysed to help us mitigate threats against the UK.

Voluntary incident response to BEIS

The BEIS Emergency Response: Capabilities and Operations (ERCO) team was established for the purpose of the coordination and response to emergencies, including cyber-attacks.

The ERCO team are contactable on a 24/7 basis (on 0300 068 6900, or erco@beis.gov.uk).

OES are encouraged to engage with ERCO in relation to any incident which requires an enduring response and resource reallocation, and which could benefit from strategic level input and support, potentially through significant cross-government cooperation and coordination.

OES are encouraged to notify the ERCO team in relation to all incidents that have or could have created a significant risk. Table 7 below provides examples of what this risk level may entail:

Table 7: Examples of what a significant risk level may entail.

Indicator	Risk level
Potential impact to the safety of the public	Consumers or members of the public have been harmed because of the incident, or it is likely that harm to individuals will be caused imminently.

Potential damages and losses	There has been a significant level of consumer detriment, environmental detriment, adverse impact on other businesses, and/or there is a prolonged disruption/denial of services, or it is possible that this impact may be caused imminently.
Complexity of remedial action	Urgent remedial action is required. Many systems could be affected, and the remedial action required takes significant resources to implement.
Public confidence	Significant loss of public/industry/international confidence in the integrity of provision of the service.
Media interest	Prolonged interest requiring significant media monitoring and frequent briefings and statements.

Glossary

Acronym	Meaning
BEIS	Department for Business, Energy, and Industrial Strategy
CAF	Cyber Assessment Framework
CNI	Critical National Infrastructure
COMAH	Control of Major Accidental Hazards
CPNI	Centre for the Protection of National Infrastructure
CSIRT	Computer Security Incident Response Team
DCMS	Department for Culture Media and Sports
DNRO	Deputy NIS Responsible Office
ERCO	Emergency Response Capabilities and Operations
GCHQ	Government Communications Headquarters
GEMA	Gas and Electricity Markets Authority
GRC	General Regulatory Chamber
HMG	Her Majesty's Government
HSE	Health and Safety Executive
IGPs	Indicators of Good Practice
NAO	NIS Accountable Officer
NCSC	National Cyber Security Centre
NIS	Network and Information Systems
NIST	National Institute for Standards and Technology
NRO	NIS Responsible Officer
OES	Operators of Essential Services
RDSPs	Relevant Digital Service Providers
SEC	Smart Energy Code
SPoC	Single Point of Contact

This publication 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.