Department for Business, Energy & Industrial Strategy

SECURITY OF NETWORK AND INFORMATION SYSTEMS REGULATION 2018

Implementation in the Energy Sector for GB

July 2018

Table of Contents

List of Annexes

Chapter 1 – About this Document

1.1. This document is for the information of those operators that will be designated as Operators of Essential Services (OES) under the UK Network and Information Systems Regulations[1] (NIS Regulations or 'the Regulations') which came into force on 10 May 2018.

1.2. This document details the responsibilities of 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, with particular focus on the first year post-May 2018. It also sets out the process and thresholds for mandatory NIS incident notifications.

1.3. This document is being provided to assist OES in the energy sector (see Chapter 3 for more information about scope and thresholds) in complying with the Regulations. We invite feedback on this document and it will be reviewed and amended as required to ensure that it remains accurate and up to date. Additional detailed guidance from Ofgem and HSE will follow this document in the coming months.

1.4. Energy is a reserved matter in Scotland and Wales and devolved to Northern Ireland. The proposed arrangements in this document therefore cover Great Britain but not Northern Ireland. OES in Northern Ireland should refer to their Competent Authority, as set out in Schedule 1 of the Regulations, for further information.

1.5. This document is structured to answer key questions that organisations may have, including:

- How the NIS Regulations and the NIS Directive are being implemented within the UK;
- Which organisations are in scope of the UK Regulations;
- Who the Competent Authorities are for the energy sector in Great Britain;
- Clarification of the role of the Competent Authority;
- The relative roles and responsibilities of the Department for Business, Energy and Industrial Strategy (BEIS), Ofgem, HSE and National Cyber Security Centre (NCSC);
- The responsibilities of OES;
- The thresholds for OES and incident reporting; and

[1] The 'Regulations' http://www.legislation.gov.uk/uksi/2018/506/contents/made

- Cyber incident response, including instructions on how OES should contact the NCSC and utilise existing emergency support structures to receive support.

1.6. This document is not formal guidance. It therefore:
- Does not create any rights enforceable at law in any legal proceedings;
- Is not a substitute for legal advice;
- Is not a set of binding instructions; and
- Does not limit the right of BEIS, Ofgem and HSE to make their own judgements or establish their own processes in accordance with the NIS Regulations.

1.7. Ofgem and HSE as the bodies responsible for NIS compliance and enforcement for the energy sector, will be setting out further guidance on security practices, through consultation with the sector, to support OES establishing and improving their cyber and security management system. We expect this to be available by Autumn 2018. This will include but is not limited to:
- Detail of the Competent Authorities' approach to working with OES from identification of critical systems to OES assessment of their current cyber practices, assessment of risk, development of improvement plans as and where required, monitoring and continuous improvement;
- Existing regulations for the sector and whether and how they overlap with the NIS Regulations;
- Sector specific assessment frameworks and holistic security practices (technical, people, processes and organisational).
- The frequency of OES assessments and sharing of them with the Competent Authority as well as Competent Authority inspections or third-party assessments of OES assessments and improvement plans;
- Cost recovery mechanisms;
- Further information about handling incident reporting, response and recovery; and
- Enforcement processes.

1.8. Further information will also be provided on the penalty process, including the appeals process.

1.9. Annex A contains a list of associated key documents and links that your organisation should be aware of. These include links to the EU Directive and UK Regulations, and relevant technical guidance from the NCSC.

Chapter 2 – Background to the NIS Directive

What is the NIS Directive?

2.1. The NIS Directive is the first EU-wide legislation on cyber security. It applies to those sectors which are vital for our economy and society, providing services such as the supply of electricity, oil, gas and water and the provision of healthcare and transport.

2.2. The NIS Directive was adopted by the European Parliament on 6 July 2016. EU Member States had until 9 May 2018 to transpose the Directive into domestic legislation. The UK has implemented the requirements of the NIS Directive through the Network and Information Systems Regulations 2018, which came into force on 10 May 2018.

2.3. The NIS Directive provides legal measures to boost the overall level of network and information system security in the EU by:

- Ensuring that Member States have in place a national framework to support and promote the security of network and information systems, consisting of a National Cyber Security Strategy, a Computer Security Incident Response Team (CSIRT), a Single Point of Contact (SPOC), and a national NIS Competent Authority (or authorities);
- Setting up a Cooperation Group, to support and facilitate strategic cooperation and the exchange of information among Member States.

2.4. Organisations that are identified by Member States as Operators of Essential Services (OES) will have to take appropriate and proportionate security measures to manage risks to their network and information systems OES will also be required to notify serious incidents to the relevant authority.

UK implementation

Public consultation

2.5. The Government, with the Department for Digital, Culture, Media and Sport (DCMS) as the Lead Department, set out its initial proposals for implementing the NIS Directive in a public consultation that ran from 8 August to 30 September 2017 (see Annex A). The consultation document included the Government's proposals and asked a series of questions on a range of detailed policy issues relating to transposition. In total the Government received over 350 responses across all sectors with 64 of those coming from the energy sector.

2.6. The responses to the consultation indicated, in general, that there was broad support for the proposals which were viewed as appropriate and proportionate. However, there were some core areas of concern highlighted which required

further clarity or changes to the approach. These included areas such as penalties, incident reporting, expectations in the first year and the roles and responsibilities of the Competent Authorities, SPOC and CSIRT.

2.7. DCMS published the Government's response to the consultation on 28 January 2018; it set out the overall policy for UK implementation and addresses concerns raised in the consultation (Annex A).

2.8. BEIS have engaged extensively with energy sector stakeholders to consider the requirements of the Directive and how best to make them work within the UK. We held three industry workshops during the consultation period. We have also provided regular updates at industry forums, including E3CC (Energy Emergency Executive Cyber Committee), DOCSG (Downstream Oil Cyber Security Group), OGISF (Oil and Gas Information Sharing Forum) and through EnergyUK. Energy sector stakeholders, Ofgem and HSE have been informally consulted in the preparation of defining the identification thresholds for OES and for incident reporting.

2.9. In the UK, the NIS Regulations 2018 require energy companies identified as OES to demonstrate active cyber security risk management, report incidents that disrupt energy supply, and take action to rectify those incidents. The Regulations identify a role for one or more regulatory bodies ('Competent Authority') to ensure compliance.

2.10. For the Energy Sector the Competent Authorities, as named in the Regulations, will be BEIS for the oil sector and upstream gas sector, and Ofgem and BEIS acting jointly for the electricity sector and downstream gas sector. In addition, HSE will undertake compliance and enforcement functions for the oil sector and specified sections of the gas sector on behalf of BEIS. Chapter 3 sets out more detail on roles and responsibilities of these bodies and also the role of the NCSC.

2.11. The UK Government is committed to ensuring that implementation requirements will:

- Be realistic and proportionate;
- Follow outcome-based security principles;
- Provide flexibility to be delivered with industry ownership, HMG support and appreciation of industry perspectives;
- Involve an initial/transitional phase focussed on critical system identification and company self-assessment of cyber risks; and
- Reflect transition and build up over several years.

National Cyber Security Centre

2.12. The NCSC has several critical roles to play in support of NIS Directive implementation. Under the UK NIS Regulations NCSC will be the UK's Single

Point of Contact (SPOC) and Computer Security Incident Response Team (CSIRT).

2.13. As the CSIRT, the NCSC will be responsible for incident response, including monitoring incidents, providing dynamic incident analysis and situational awareness as well as providing early warning alerts and announcements.

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

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

2.16. All these roles are advisory; the NCSC will not have any regulatory responsibilities. It will not be able to, or seek to, enforce any actions on an OES. Enforcement will solely be the responsibility of the Competent Authorities.

The NIS Cyber Security Principles and Guidance Collection

2.17. This comprises a set of outcome-based security principles which form part of the core requirements placed on OES 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. The NCSC published this guidance in parallel to the response to the consultation on 28 January 2018. Further detail can be found in Chapter 4 and Annex A provides a link.

The Cyber Assessment Framework (CAF)

2.18. This tool provides a systematic method for assessing the extent to which OES are achieving the outcomes specified by the NIS principles. It can be used by Competent Authorities when assessing OES or by OES themselves as a self-assessment tool. The CAF will provide statements of good and bad practice against each element of the security principles. This will enable assessment of the maturity of an OES against each element. An initial version of the CAF was published 30 April 2018 and guidance on its use in demonstrating compliance will be provided by Competent Authorities. The CAF will be developed further in the coming months in collaboration with industry, for a likely update to the CAF by NCSC in Autumn 2018. **OES should contact their Competent Authority if they are interested in volunteering to take part in an NCSC-supported pilot**

exercise of applying the CAF.

2.19. The CAF will be used to assess compliance for companies who are in scope of NIS, except for those aspects of OES services which fall within the scope of the requirements laid out in in the Smart Energy Code (SEC). Ofgem are minded to accept compliance with the relevant security provisions of the SEC and Suppliers licences as being sufficient for compliance with regulation 10 of NIS, although this will be confirmed in due course.

Chapter 3 – Implementation in the Energy Sector

Who is in scope?

3.1. The EU NIS Directive specifies the types of entities that all Member States should consider for inclusion (Annex II of the NIS Directive). In the UK, designation of organisations as OES is set by thresholds in the Regulations relating to the scale of an organisation's operations and these thresholds came into force on 10 May 2018. These thresholds have been defined based on the level of societal or economic impact which could result from disruption to the services those entities provide. Organisations that meet these thresholds will automatically be designated as OES and therefore required to comply with the Regulations. The definitions and thresholds for designating OES are set out in the NIS Regulations (see Annex A for a link to the Regulations and Annex E for the table of OES thresholds).

3.2. BEIS recognise that our energy system is changing. There are more distributed and localised energy resources as well as increasing use of smart, more flexible energy technologies such as demand side response and storage. Government is committed to ensuring that good cyber security practices are adopted across the energy sector including for newer technologies. BEIS will be undertaking further work together with Ofgem and industry to more fully understand how the Regulations might be applied to emerging energy technologies and systems over the longer term.

Designation and Revocation of OES

3.3. Organisations that meet the OES thresholds are designated as OES and are in scope of the NIS Regulations. **Under regulation 8(2), it is the responsibility of the OES to determine whether they are in scope and to then notify their relevant Competent Authority by 10 August 2018.** If an OES is not sure whether they are in scope of the NIS Regulations, it is their responsibility to contact the relevant Competent Authority to clarify whether they are in scope. See Annex D for contact information.

3.4. In order to raise awareness of the NIS Regulations in the first transitional implementation year, BEIS has written out to companies that we believe are in scope.

3.5. Our overarching approach for implementation is one of collaboration, between OES and Ofgem or HSE. Therefore, Competent Authorities and OES should be proactive in engaging with each other.

3.6. The Regulations include additional powers for a Competent Authority to designate an OES or to revoke a designation, under certain circumstances.

3.7. The designation power (regulation 8) may be used in circumstances where an entity does not meet the threshold for designation as an OES, but the Competent Authority concludes that a security incident affecting the provision of that essential service by that entity would have significant disruptive effects on the provision of the essential service. This designation power will only be used as an exception to bring in select essential service operators.

3.8. Regulation 9 contains the power for a 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. Whilst every care has been taken in development of the thresholds, and these have been aligned wherever possible to existing thresholds and consulted on with industry, Government recognises that it is necessary to include such a power as a backstop.

If my company is an OES how do I identify which of my systems are in scope?

3.9. It is a matter for individual OES to identify which of their systems are critical for provision of their essential service. The Competent Authority will not specify which systems are in scope but it may request an OES to share the list of systems which could cause disruption to an essential service if compromised and the process followed in identifying such systems. The Competent Authority may challenge the systems identified should it believe areas or systems are missing that could be critical for the provision of the essential service. NCSC are also developing guidance that should help operators to identify critical systems.

Are supply chain companies in scope?

3.10. BEIS does not anticipate that companies in the supply chain of OES will be deemed to be directly in scope. However, where supply chain companies could cause disruption to the provision of the essential service by the OES, the OES may need to ensure that these companies have sufficient security standards as part of their duties under regulation 10.

3.11. Competent Authorities may require OES to provide information relating to their supply chain under regulation 15(2) and consider this as part of their inspections under regulation 16. Companies should seek their own legal advice on this matter as needed.

3.12. As a matter of good practice OES are strongly encouraged to consider the NIS security principles in their procurement process and use NCSC guidance to underpin support arrangements with suppliers. NCSC have set out guidance on

supply chain related security considerations (Objective A4 Supply Chain principle, see Annex A for link to NCSC guidance) that should be addressed where relevant to the provision of the essential service.

Roles and Responsibilities

Who will be the Competent Authority for the energy sector in Great Britain?

3.13. For the energy sector in England, Wales and Scotland, BEIS is named in the Regulations as the Competent Authority – jointly with Ofgem for downstream gas and electricity. For upstream and downstream oil and for upstream gas, BEIS is named as the Competent Authority but the compliance functions will be carried out under an Agency Agreement by HSE.

3.14. This means that BEIS will remain 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 will be carried out by Ofgem and HSE, with the exact approach depending on the sub-sector.

3.15. The Competent Authority for each energy sub-sector is set out in Table 1 below.

Sub-Sector	Competent Authority (GB)
Electricity	**Ofgem** (acting jointly with The Secretary of State for BEIS)
Gas	Gas storage facilities, LNG facilities, gas processing facilities and petroleum production projects – BEIS with compliance functions carried out by **HSE** under an Agency Agreement. Otherwise, **Ofgem** (acting jointly with The Secretary of State for BEIS)
Oil	BEIS with compliance functions carried out by **HSE** under an Agency Agreement.

Responsibilities of BEIS Competent Authority Function

3.16. The BEIS regulatory policy team will be responsible for:

- Setting thresholds for OES and incident reporting;
- Designation and revocation of OES;
- Raising industry awareness of NIS compliance requirements;
- Ensuring alignment of approach across the energy sector;
- Setting policy on any incremental increase of initial compliance requirements over time;
- Reviewing frameworks with HSE and Ofgem; and
- Monitoring the overall cyber security ‘health’ of the energy sector.

Responsibilities of Ofgem and HSE

3.17. Ofgem and HSE will be responsible for:

- Monitoring the application of the NIS Regulations in their sector;
- Preparing and publishing guidance on security practices and systems management approaches to assist OES in meeting the requirements of the NIS Regulations;
- Assessing compliance of OES against the requirements of the NIS Regulations, including using inspections and third-party assessments;
- Cooperating with other Competent Authorities to provide consistent advice and oversight to OES;
- Receipt of incident reports;
- Ensuring processes are in place by an OES for incident response for non-cyber incidents;
- Incident investigation; and
- Enforcement of the requirements of the NIS Regulations including how penalties will be issued.

3.18. More detail on the Ofgem and HSE role will be provided in the upcoming Competent Authority guidance.

BEIS also undertakes voluntary collaboration, how will that work in future?

3.19. BEIS undertakes voluntary collaboration work on energy cyber security and wider energy resilience to further national security objectives. This work will continue as we consider it important in helping to understand, mitigate and respond to cyber threats; and to build capability in the energy sector.

3.20. The BEIS Energy Cyber Security Team have also established a new regulatory policy team within the Energy Development and Resilience Directorate. It will oversee regulatory policy and international liaison and liaise with Ofgem and HSE. This is the team referred to in paragraph 3.16.

3.21. The BEIS voluntary and regulatory energy cyber security policy teams are operating separately from each other with split roles and responsibilities. We are also operating strict information management protocols to ensure that no information shared as part of voluntary collaboration is used for regulatory purposes. The regulatory policy staff have not previously worked on voluntary collaboration and have no access to this information.

3.22. Information about an organisation's cyber security obtained by the BEIS voluntary collaboration and resilience teams will not normally be passed on to the regulatory policy team or used for regulatory purposes unless the organisation has expressly consented. However, BEIS retains the right to engage with a regulator where inaction poses an immediate threat to life, national security or public safety.

NCSC

3.23. The UK NIS Regulations name The Government Communications Headquarters (GCHQ) as the CSIRT and the SPOC. The NCSC, a part of GCHQ, will carry out these functions. NCSC is the UK technical authority on cyber security, and in this capacity, it is supporting both Competent Authorities and OES in a number of different ways, including by developing a set of cyber security principles and a collection of supporting guidance intended to assist organisations responsible for cyber security in relation to NIS essential services. It has also developed an initial version of the CAF aimed at providing a structured approach to assessing the extent to which an OES is meeting the NIS cyber security principles. NCSC has no regulatory responsibilities under the NIS Regulations.

Who do I contact with energy related NIS implementation questions?

3.24. Annex D sets out useful contact details at BEIS, Ofgem and HSE. Whilst NIS brings cyber security resilience into the regulatory space it is not intended to replace existing structures. Companies are encouraged to contact BEIS voluntary teams and the NCSC under existing arrangements and about non-NIS incidents. The Cyber Security Information Sharing Partnership (CiSP) portal provided by NCSC remains an important source of advice for OES; regulators do not have access to this platform. Who to contact in the event of a non-NIS incident is covered in Chapter 4 and also Annex H.

Chapter 4 - Requirements on Operators of Essential Services (OES)

Security requirements

4.1. The NIS Regulations require OES to:

- Manage risks posed to the security of the network and information systems on which their essential service relies;
- Report to the Competent Authority any incident which has a significant impact on the continuity of the essential service which that OES provides (see the incident reporting thresholds that BEIS has devised); and
- Take actions to rectify those incidents.

4.2. The BEIS approach taken to setting the security requirements for OES is one based on principles and guidance. The NCSC has defined a set of cyber security principles consisting of 14 top-level outcomes, with supporting narrative, which are grouped into four high-level objectives (see Annex A and Annex B). These principles should be relevant to all network and information systems supporting the delivery of essential services for Energy, Transport, Health, Drinking Water Supply and Distribution and Digital Infrastructure. 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 sector context.

4.3. 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 can lead to unintended consequences, misallocation of resource and limited benefit. Organisations understand their own business better than any external entity and should take informed, risk balanced decisions about how they achieve the outcomes specified by the principles.

4.4. It is for OES to demonstrate compliance with the Regulations by putting in place appropriate and proportionate security arrangements. To support 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 need to consider when deciding how to achieve the outcome and recommends some ways to tackle common cyber security challenges.

4.5. NCSC have produced a Cyber Assessment Framework (CAF), which can be

used to determine whether an OES is achieving the outcomes set out in the NIS security principles, unless those services are already covered within the existing compliance scope of the Smart Energy Code (SEC) as described in 2.19.

4.6. The NIS Regulations and security requirements will not replace existing regulatory duties. For those aspects of OES services which fall within the scope of the requirements laid out in in the SEC, Ofgem are minded to accept compliance with the relevant security provisions of the SEC and Suppliers licences as being sufficient for compliance with regulation 10 of NIS, although this will be confirmed in due course.

4.7. The NCSC security principles and the Cyber Assessment Framework are linked in Annex A. The NCSC's principles and guidance are primarily focused on ensuring baseline cyber security risk management. However, **OES will also need to consider broader resilience risks when considering 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 and environmental hazards. Examples of resources and guidance to consider in relation to broader resilience risks are provided in Annex C.

Transitional Period – from May 2018

4.8. BEIS views May to end 2018 as a familiarisation and transitional period for energy Competent Authorities and OES. We recognise that there are commercial costs associated with compliance, that the information provided through the CAF will be new to some organisations and that not all sector specific information will be available from May. Therefore there will naturally need to be a gradual transition before OES are able to clearly demonstrate that they are meeting the NIS security principles.

4.9. There are several ways that OES can take action to prepare from May 2018 onwards. These include:

- Ensuring that they are familiar with the Regulations, NCSC Security Principles and Guidance collection and the Cyber Assessment Framework;
- **Determine whether they are in scope and notify their relevant Competent Authority by 10 August 2018**. If an entity is not sure whether their organisation is in scope of the NIS Regulations, it is their responsibility to contact the relevant Competent Authority to receive that assurance.
- Identifying network and information systems which are in scope of the Regulations and agreeing this with the Competent Authority;
- Commence self-assessment against the Cyber Assessment Framework, liaising with their Competent Authority but noting the CAF is currently in initial form and will be developed further and finalised in the coming months.

Early and ongoing engagement by the OES with their relevant Competent Authority is therefore essential.

- Identifying areas for improvement consistent with the principles and guidance set by NCSC to ensure appropriate and proportionate measures are established to protect these networks and information systems;
- Reviewing arrangements for incident reporting under NIS, and **where appropriate report any NIS Incidents to the Competent Authority from 18 May 2018** (See Incident Notification in this Chapter); and
- **Providing the name of your NIS Responsible Officer (your main point of contact for NIS) to BEIS as soon as possible**. This 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 BEIS and Ofgem or HSE. 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. Ofgem and HSE will set out further details in due course.

Year One - 2019

4.10. Full instructions on how and when an OES should complete assessments will be set out in further guidance from Ofgem and HSE due in Autumn 2018.

4.11. By early 2019 (or earlier if completed) BEIS expects an OES to have undertaken their initial self-assessment using the CAF and submitted this with evidence to their relevant Competent Authority for review.

4.12. OES should also submit their improvement plan to address any shortcomings and risks that they identified through the assessment. These assessments and improvement plans will be reviewed by the Competent Authority and discussed with the OES, where necessary.

Year Two - 2020

4.13. By early 2020, once a baseline level of security has been established by OES, BEIS expects the Competent Authority to monitor the delivery of improvement plans, and periodically seek further assessments of compliance, overseen and directed by the Competent Authority on a rolling basis.

4.14. For the upstream and downstream oil sectors and upstream gas sector, following the review of OES assessments it is expected that HSE may follow up the conclusions of the review and improvement plans through planned intervention activity.

4.15. For the electricity and downstream gas sectors it is expected that Ofgem will require companies to appoint an independent third party from a list of

accredited suppliers to carry out a review of the self-assessments they undertake. Improvement plans would also be validated as appropriate by the third party.

4.16. Further information on both HSE and Ofgem's proposed approaches will be provided in their upcoming guidance.

The Future

4.17. Effective cyber security of network and information systems is essential to protect critical national infrastructure and enabling an energy system for decades to come. Whilst recognising that companies are starting from varying baselines, BEIS expect there to be a gradual increase towards a higher level of compliance with the NIS security principles over time. Any raising of requirements will be determined through consultation with industry and the Competent Authorities.

How will an OES know what Ofgem/HSE's expectations and arrangements for compliance and monitoring are?

4.18. Ofgem and HSE will be assessing the compliance of operators regarding the requirements of the NIS Regulations. Compliance will be assessed against the 14 principles laid out in the NIS Consultation and published on the NCSC's website. The link to these documents can be found at Annex A and Annex B.

4.19. Ofgem and HSE plan to publish their own guidance for assessment of OES compliance with the security requirements of NIS by Autumn 2018. BEIS expect this information to be published for the assessment process to be transparent and to ensure that OES understand what compliance looks like.

What approach will be taken to risk management, how flexible will you be?

4.20. The requirements of the NIS Regulations centre on appropriate risk management. BEIS recognise that even at more sophisticated levels of cyber security, OES cannot mitigate against all risk.

4.21. The Competent Authorities will be looking at OES adherence to the application of NIS security principles. They will engage in a dialogue with OES to understand vulnerabilities in critical systems and any mitigating factors that should be considered. OES will be required to demonstrate compliance using the CAF and associated guidance published by the Competent Authority.

4.22. Risk management decisions are for companies to determine based on their risk appetites and internal management and audit processes, provided that their approach complies with the NIS Regulations. An OES will need to be able to justify their approach and describe any risk management decisions to their

Competent Authority.

Who will pay for compliance activity?

4.23. For the purposes of carrying out a Competent Authority inspection or third party assessment, the OES will be asked to pay the reasonable costs of this work. The NIS Regulations include a power to permit Competent Authorities to recoup reasonable costs from those that they regulate (see Part 6 of the Regulations). The Competent Authorities processes and regimes to recoup reasonable costs will be set out in greater detail in HSE and Ofgem's further guidance.

Incident notification

4.24. 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.

4.25. The high-level incident reporting requirements applied as soon as the NIS Regulations come into force on 10 May 2018. However, BEIS recognised that this was new information for many operators in the energy sector and informed OES contacts that in practice we did not expect operators to comply with these requirements until 18 May 2018.

4.26. The way that the UK has chosen to interpret this requirement is to make a distinction between:

- Reporting for incident management purposes (which, while strongly recommended, will continue on a **voluntary** basis); and
- **Mandatory** notifications under NIS Regulations (which are only required when the level of disruption caused by an **incident meets the specified threshold** (as set out at Annex F).

4.27. We are making this distinction because we want OES to seek 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 very different objectives to the reporting requirements specified by the NIS Regulations.

4.28. **Details of voluntary incident reporting for cyber non-NIS incidents are set out at Annex H.**

What is a NIS reportable incident?

4.29. The requirement to report NIS incidents, under regulation 11, applies when both the below are fulfilled:

- The incident has an actual adverse effect on the security of network and information systems.
- The incident has a significant impact on the continuity of the essential service which that OES provides.

4.30. A 'significant impact' is where there is a reduction or degradation of an essential service, at a magnitude equivalent to or above the sector specific incident thresholds set out in Annex F.

What is the process for NIS incident notification?

4.31. If a NIS reportable 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. The notification should be in the form of an email to the Competent Authority. A template is set out in Annex G (which reflects the information requirements of the Regulations) and contact details can be found in Annex D. It is not a regulatory requirement that OES use this template, but it may be helpful in the interim prior to Ofgem and HSE publishing detailed guidance.

4.32. As a minimum, in determining the significance of an incident OES should have regard to the following (as set out in the Regulations):

- the number of users affected by a disruption to an essential service;
- the duration of the incident, and;
- the geographical area affected.

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

4.34. Operators should also ensure they are following the NIS incident response and recovery guidance as outlined in principle D1 (see Annex B).

I have an incident below the NIS threshold. Should I still report this and who to?

4.35. OES should continue to report incidents, using existing reporting mechanisms where established. OES are encouraged to report cyber incidents to BEIS and NCSC, following the guidelines set out in Annex H, to enable government to provide support where required and identify any emerging trends across the sector. The Competent Authorities should only be notified of NIS incidents unless an OES wishes to inform them as part of their developing relationship.

How will Government handle NIS related incident response in the Energy Sector?

4.36. The incident response process for NIS incidents is similar to existing response processes. When an OES reports an incident, Ofgem and HSE will have the responsibility to:

- Check if the OES has been in contact with the NCSC and the BEIS voluntary team for incident response support in the case of cyber incidents;
- Remind the OES to use existing emergency structures for incident response support in the case of non-cyber incidents, including reporting to the BEIS energy resilience team;
- Inform the CSIRT if the incident has affected other Member States so that information can be shared;
- Monitor the incident as necessary; and
- If appropriate, and liaising with BEIS if necessary depending on sub-sector, disseminate information for relevant stakeholders, including other OES, about the incident, including giving them incident warnings; and conduct incident investigations.

Incident investigation

Who will investigate NIS related incidents in the Energy Sector and how will they do it?

4.36. There is no requirement to investigate every incident and this decision will be a matter for the Competent Authority.

4.37. The purpose of an investigation is to:

- 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.

4.38. An incident is not in itself a breach of the NIS Regulations and therefore does not automatically mean enforcement action will be taken. If OES have assessed the risks adequately, taken appropriate security measures, engaged 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 thresholds would however be an infringement of the NIS Regulations.

Chapter 5 – Competent Authority Approach

Information available to the Competent Authority

5.1. The Competent Authority is able to request information from OES in order to fulfil its regulatory duties (Regulations 15-16).

5.2. Competent Authorities will also receive support from the NCSC to undertake their responsibilities. For example, Competent Authorities will likely prioritise according to sector risk assessments, and NCSC could hold information that can be part of that risk assessment. In this case, information could be provided in aggregated form, or anonymised in order not to call out individual organisations. Once an incident is closed, to ensure any regulatory investigations are well informed, balanced and accurate, NCSC may provide technical expertise to verify findings.

Enforcement Regime

5.3. Oversight and enforcement of the NIS Regulations is the responsibility of the designated Competent Authority. For energy Ofgem and HSE will be developing detailed guidance on the enforcement framework for NIS requirements in their sub-sectors.

How will Enforcement and Penalties work in practice for an OES?

5.4. The UK Regulations provide some information, but the exact enforcement and penalties process and actors involved will be set out in further guidance.

5.5. Enforcement will be a stepped approach, a collaborative approach between the Competent Authority and OES would be the preferred procedure. Where this is unsuccessful and there are clear failings not being addressed or where the OES has been negligent in its application of the requirements then the Competent Authority may issue a formal enforcement notice.

5.6. If an OES fails to take action to rectify a failure identified by an enforcement notice or if they are in clear breach of the NIS Regulations the Competent Authority may issue a penalty notice. Issuing a monetary penalty is a last resort. Penalties must be appropriate and proportionate to the breach.

5.7. BEIS expect that Ofgem and HSE will take a cautious approach to enforcement for the first year. The focus in the transitional period will be on working with OES to ensure compliance rather than on enforcement. This does not mean that a Competent Authority cannot consider penalties during the first year of the implementation, for example, if it is the case an OES is considered to have severely breached the Regulations in the implementation of security measures or the handling of an incident. However, enforcement must be proportionate and appropriate. The Government recognises that some leeway must be given during

the transitional period whilst OES are familiarising themselves with the requirements of the NIS Regulations.

What considerations will a Competent Authority make before taking enforcement action?

5.8. Before taking enforcement action under the NIS Regulations, a Competent Authority must consider whether it is reasonable and proportionate based on the facts to take such action. The following factors are likely to be relevant:

- Any representations made by the OES;
- Any steps taken by an OES towards complying with the requirements set out in the Regulations;
- Any steps taken by an OES for remedying the consequences of any non-compliance with the requirements set out in the Regulations;
- Whether the OES has had adequate time to implement the requirements of the Regulations; and
- Whether a failure to implement has also occurred under other UK or EU legal requirements and any penalties that may be applied under that requirement.

Chapter 6 – What do I need to know about the other aspects of the Directive?

How will National and International co-operation work?

National

6.1. Where there are operators that provide essential services to more than one sector, and therefore fall under the remit of more than one Competent Authority, the relevant Competent Authorities are encouraged to cooperate and provide consistent advice and oversight.

6.2. Competent Authorities are encouraged to work with other regulators outside the NIS Regulations, with the aim of avoiding duplication where possible of such requirements as incident reporting, inspections and compliance activities.

6.3. Competent Authorities should also work closely with other regulators to ensure that, where an incident has contravened more than one set of regulations, the cumulative impact of multiple penalties from different regulators doesn't result in a disproportionate or punitive overall penalty.

International

6.4. The Department for Digital, Culture, Media and Sport (DCMS) is the UK representative at the EU NIS Cooperation Group. This Group was established to support and facilitate strategic cooperation between the EU Member States regarding the security of network and information systems. The Cooperation Group is composed of representatives of EU Member States, the European Commission, and the European Union Agency for Network and Information Security (ENISA).

6.5. The NCSC will liaise with relevant authorities in other EU Member States, as part of its role as the SPOC.

6.6. The SPOC is required to submit annual report of NIS incidents to the EU. On a biennial basis the SPOC must report the number of OES and the thresholds for identification to the EU.

Chapter 7- Forward Timeline

7.1. As set out in Chapter 4, BEIS views 2018 as a transitional period during which OES will familiarise themselves with the NIS requirements and undertake self-assessments.

7.2. There are several key dates that operators of essential services (OES) should be aware of:

- **From May 2018**:
  - OES identify whether they are in scope of the NIS Regulations and contact the relevant Competent Authority;
  - OES identify network and information systems which are in scope of the Regulations;
  - OES familiarise themselves with the Cyber Assessment Framework (CAF) and commence self-assessments; and
  - OES identify areas for improvement that have been flagged through the CAF and are consistent with the principles and guidance set by NCSC and develop improvement plans.

- **November 2018:**
  - Competent Authorities will work with BEIS, NCSC and industry to develop any sector specific security guidance and associated assessment tools as necessary. Publication of the guidance by Competent Authorities will provide information on the deadline for completion of self-assessments and submission of improvement plans in due course (as detailed above).
  - UK to complete identification of OES.

- **From Q2 2019 or potentially earlier depending on the CA:**
  - Competent Authorities will review the self-assessment evidence and improvement plans; and
  - Competent Authorities will establish a rolling programme of inspections or third-party assessments/validations of OES own self-assessments.

- **By May 2020:** DCMS will review the Regulations and publish a report. At this point there may be an opportunity to adjust the thresholds for OES.

7.3. During the period 2018-2020, BEIS and NCSC will continue our programme of voluntary engagement and dialogue with industry on non-NIS related energy cyber security activities.

Annex A - Key documents relating to the Security of Network and Information Systems Directive and the UK Regulations

Document	Web link
UK Network and Information Systems Regulations 2018	http://www.legislation.gov.uk/uksi/2018/506/contents/made
DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union	http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
UK Government NIS consultation	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/636207/NIS_Directive_-_Public_Consultation__1_.pdf
UK Government NIS consultation response	https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive
NCSC NIS Guidance Collection	https://www.ncsc.gov.uk/guidance/nis-guidance-collection Security Principles: https://www.ncsc.gov.uk/guidance/table-view-principles-and-related-guidance
NCSC Cyber Assessment Framework:	https://www.ncsc.gov.uk/guidance/nis-directive-cyber-assessment-framework
UK National Cyber Security Strategy 2016- 2021	https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
EU Commission NIS Cooperation Group	https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

Annex B - The NIS security principles

The implementation of Article 14 of the NIS Directive is described via 4 top-level objectives. The objectives will be realised through implementation of 14 sector-agnostic security principles devised by the NCSC. Each principle describes mandatory security outcomes to be achieved. The full guidance collection on the NCSC's website (see Annex A) goes into further detail on each principle with references to a range of existing guidance and standards.

Objective A: Managing security risk

Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services.

A1. Governance

Putting in place the policies and processes which govern your organisation's approach to the security of network and information systems.

A2. Risk management

Identification, assessment and understanding of security risks. And the establishment of an overall organisational approach to risk management.

A3. Asset management

Determining and understanding all systems and/or services required to maintain or support essential services.

A4. Supply chain

Understanding and managing the security risks to networks and information systems which arise from dependencies on external suppliers.

Objective B: Protecting against cyber attack

Proportionate security measures are in place to protect essential services and systems from cyber-attack.

B1. Service protection policies and processes

Defining and communicating appropriate organisational policies and processes to secure systems and data that support the delivery of essential services.

B2. Identity and access control

Understanding, documenting and controlling access to essential services systems and functions.

B3. Data security

Protecting stored or electronically transmitted data from actions that may cause disruption to essential services.

B4. System security

Protecting critical network and information systems and technology from cyber attack.

B5. Resilient networks and systems

Building resilience against cyber-attack.

B6. Staff awareness and training

Appropriately supporting staff to ensure they can support essential services' network and information system security.

Objective C: Detecting cyber security events

Capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services.

C1. Security monitoring

Monitoring to detect potential security problems and track the effectiveness of existing security measures.

C2. Proactive security event discovery

Detecting anomalous events in relevant network and information systems.

Objective D: Minimising the impact of cyber security incidents

Capabilities to minimise the impact of a cyber security incident on the delivery of essential services including the restoration of those services where necessary.

D1. Response and recovery planning

Putting suitable incident management and mitigation processes in place.

D2. Lessons learned

Learning from incidents and implementing these lessons to make a more resilient service.

Annex C - Broader resilience risks to network and information systems

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.

C.1 CPNI website

https://www.cpni.gov.uk/network-and-information-services-nis

A useful resource for all organisations is the CPNI website which contains advice and guidance on many aspects of physical and personnel security.

C.2 Technical guidelines for the implementation of minimum security measures for Digital Service Providers

https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

This document was produced by the European Union Agency for Network and Information Security (ENISA) to define the common baseline security objectives for Digital Service Providers under the NIS Directive. It describes different levels of sophistication in implementing those objectives and maps the objectives against other well-known industry standards, guidance and frameworks.

Whilst this has been developed for DSPs there are sections that are also relevant to OES. It contains two sections specifically on managing broader resilience risks:

SO 08 – Physical and environmental security

The DSP establishes and maintains policies and measures for physical and environmental security of data centres such as physical access controls, alarm systems, environmental controls and automated fire extinguishers etc.

SO 09 – Security of supporting utilities

The DSP establishes and maintains appropriate security measures to ensure the security of supporting utilities such as electricity, fuel, HVAC etc. For example, this may be through the protection of power grid connections, diesel generators, fuel supplies, etc.

C.3 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.

C.4 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 organisation in managing cyber risks. It was called for in a US Executive Order. The Framework Core 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.

Annex D - Helpful Contacts

Body	Contact point
BEIS Regulatory Policy Team	nis.energy@beis.gov.uk
Ofgem	Generic: cybersecurityteam@ofgem.gov.uk NIS incident reporting: cyberincident@ofgem.gov.uk
HSE	NIS.Cyber.Incident@hse.gov.uk

Annex E - OES Thresholds for the Energy Sector[2]

Subsector	Essential service	Identification threshold[3]
Electricity	Electricity supply	In Great Britain: 1) Electricity undertakings that carry out the function of supply to more than 250,000 final customers. 2) Electricity undertakings that: ● carry out the function of supply; and ● carry out the function of generation via generators that, when cumulated with the generators of affiliated undertakings, would have a total capacity[4], in terms of input to a transmission system, greater than or equal to two gigawatts. For the purposes of this threshold: ● generators that are not connected to a transmission system are excluded; ● nuclear electricity generators are excluded.
	Electricity transmission	In Great Britain: 1) Transmission system operators with a potential to disrupt delivery of electricity to more than 250,000 final customers. This threshold shall not take into account those transmission systems for which an offshore transmission licence or interconnector licence applies. 2) Holders of offshore transmission licences where the offshore transmission systems of that licence

[2] Definitions of the terms used in the table are set out in the NIS Regulations.
[3] In setting these thresholds it is not BEIS intention to capture operators who are currently non-operational
[4] Where “Capacity” refers to “Transmission Entry Capacity” as defined in National Grid’s Connection and Use of System Code (CUSC)

		holder and its affiliated undertakings are directly connected to generators that have a total cumulative capacity[5], in terms of input to a transmission system, greater than or equal to 2 gigawatts. 3) Holders of interconnector licences where the electricity interconnector to which the licence relates has a capacity[6], in terms of input to a transmission system, greater than or equal to 1 gigawatt.
	Electricity distribution	In Great Britain: Distribution system operators with the potential to disrupt delivery of electricity to more than 250,000 final customers.
Oil	Conveyance of oil through a relevant upstream petroleum pipeline	The operator of a relevant upstream petroleum pipeline which has a throughput of more than 3,000,000 tonnes of oil equivalent per year excluding natural gas, who is not designated an operator of essential services in relation to this pipeline under another threshold requirement.
	Oil transmission pipeline	In Great Britain: Operators of any pipeline with throughput capacity of more than 500,000 tonnes of crude oil-based fuel per year.
	Operation of relevant oil processing facilities	In the case of: ● a relevant oil processing facility; or ● a relevant upstream petroleum pipeline which is connected to and operated from a relevant oil processing facility, an operator of a facility or pipeline with a throughput of more than 3,000,000 tonnes of oil equivalent per year.
	Oil production, refining, treatment, storage and transmission:	In Great Britain: Operators of any facility where that facility has a capacity greater than any of the following values:

[5] Where “Capacity” refers to “Transmission Entry Capacity” as defined in National Grid’s Connection and Use of System Code (CUSC)

[6] Where “Capacity” refers to “Transmission Entry Capacity” as defined in National Grid’s Connection and Use of System Code (CUSC)

		(i) storage of 500,000 tonnes of crude oil based fuel; (ii) production of 500,000 tonnes of crude oil-based fuel per year; (iii) supply of 500,000 tonnes of crude oil-based fuel per year.
	Operation of petroleum production projects other than projects which are primarily used for the storage of gas	In the case of: ● a relevant offshore installation which is part of a petroleum production project other than a project which is primarily used for the storage of gas; or ● a relevant upstream petroleum pipeline which is connected to and operated from such an installation, an operator of an installation or pipeline with a throughput of more than 3,000,000 tonnes of oil equivalent per year.
Gas	Gas supply	In Great Britain: Supply undertakings that supply gas to more than 250,000 final customers.
	Gas transmission	In Great Britain: 1) Transmission system operators with a potential to disrupt delivery to more than 250,000 final customers. This threshold shall not take into account those transmission systems for which an interconnector licence applies. 2) Holders of interconnector licences where the gas interconnector to which the licence relates has the technological capacity[7] to input more than 20 million cubic metres of gas per day to a transmission system.
	Gas distribution	In Great Britain: Distribution system operators with a potential to disrupt delivery to more than 250,000 final customers.

[7] Where “Technological Capacity” refers to the Deliverability of the interconnector

	Operation of gas storage facilities	In Great Britain: Storage system operators where the storage facility has the technological capacity[8] to input more than 20 million cubic metres of gas per day to a transmission system.
	Operation of LNG facilities	In Great Britain: LNG system operators where the LNG facility has the technological capacity[9] to input more than 20 million cubic metres of gas per day to a transmission system.
	Operation of relevant gas processing facilities	In the case of: • a relevant gas processing facility; or • a relevant upstream petroleum pipeline which is connected to and operated from a relevant gas processing facility, an operator of a facility or pipeline with a throughput of more than 3,000,000 tonnes of oil equivalent per year.
	Operation of petroleum production projects other than projects which are primarily used for the storage of gas	In the case of: • a relevant offshore installation which is part of a petroleum production project (other than a project which is primarily used for the storage of gas); or • a relevant upstream petroleum pipeline which is connected to and operated from such an installation, an operator of an installation or pipeline with a throughput of more than 3,000,000 tonnes of oil equivalent per year.

[8] Where “Technological Capacity” refers to the Deliverability of the facility
[9] Where “Technological Capacity” refers to the Deliverability of the facility

Annex F - Incident Reporting Thresholds

BEIS have worked with Ofgem and HSE to set incident reporting thresholds aligning, wherever possible, with other reporting arrangements that are already in place. We will be monitoring the application of the thresholds over time and through discussions with industry to ensure that they are fit for purpose.

NIS Incident Reporting Thresholds for Electricity and Downstream Gas

Sector	Incident Threshold	Aligns with
Gas Transmission	Loss of supply or outage that has or is likely to lead to loss of supply to offtakes and affects customers.	Current Ofgem reporting requirement
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.	Current Ofgem reporting requirement
Gas Distribution	Unplanned single incident loss of supply to 5,000 customers.	Current Ofgem reporting requirement
Electricity Distribution	Unplanned single incident loss of supply to 50,000 customers for more than 3 minutes.	Current Ofgem reporting requirement
Gas Interconnectors	Unplanned loss of ≥10MCM over a 24-hour period.	Upstream Gas Production, Processing and LNG/Gas Storage thresholds, which are aligned to existing OGA reporting thresholds.
Electricity Interconnectors	The net unauthorised or unplanned loss or gain of ≥560MW of interconnector flow in a given direction.	Incidents that have the potential to impact the delivery of electricity to end customers
Electricity Generation	The unauthorised or unplanned loss of ≥1500MW of electricity generation, when cumulated with all generators operated by affiliated undertakings. This includes generation scheduled to dispatch within the next 4 hours.	Incidents that have the potential to impact the delivery of electricity to end customers
Energy Suppliers	Unplanned shut off or single incident loss of supply to 50,000 customers for more than 3 minutes.	Electricity distribution operator threshold.

In the Downstream Gas & Electricity sector, the NIS incident reporting thresholds have predominantly been aligned with existing Ofgem reporting thresholds for electricity and gas transmission and distribution. For electricity generation and interconnectors, where equivalent requirements are not currently in place, thresholds have been designed to capture incidents that have the potential to significantly impact the delivery of electricity to end customers. For gas interconnectors, the incident reporting threshold has been aligned to other essential services that provide gas input into the National Transmission System (e.g. LNG and Gas Storage).

NIS Incident Reporting Thresholds for Downstream Oil

Sector	Incident Threshold	Aligns with
Oil transmission by pipeline	Loss of >[20]% of supply for >24 hours.	Downstream oil resilience policy
Operators of oil production refining and treatment facilities, storage and transmission.	Loss of >[20]% of supply for >24 hours.	Downstream oil resilience policy

NIS Incident Reporting Thresholds Upstream Oil and Gas

Sector	Incident Threshold	Aligns with
Conveyance of oil through relevant upstream petroleum pipelines	Unplanned loss of conveyance > 8,219 tonnes oil equivalent over 24-hour period	Existing BEIS Guidance for terminal operators – oil and gas AND NIS Threshold for inclusion – level at which there is a potential impact to supply.
Operation of relevant oil processing facilities	Unplanned loss of conveyance > 8,219 tonnes oil equivalent over 24-hour period	Existing BEIS Guidance for terminal operators – oil and gas AND NIS Threshold for inclusion – level at which there is a

		potential impact to supply.
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	Existing BEIS Guidance for terminal operators – oil and gas AND NIS Threshold for inclusion – level at which there is a potential impact to supply.
Operation of gas storage facilities	Unplanned loss of >10MCM (or 8,219 tonnes oil equivalent) over 24-hour period.	Thresholds for production and processing of gas.
Operation of LNG facilities	Unplanned loss of >10MCM (or 8,219 tonnes oil equivalent) over 24-hour period.	Thresholds for production and processing of gas.
Operation of relevant gas processing facilities	Unplanned loss of conveyance > 8,219 tonnes oil equivalent over 24-hour period	Existing BEIS Guidance for terminal operators – oil and gas AND NIS Threshold for inclusion – level at which there is a potential impact to supply.

- For upstream oil and gas, in consultation with the Oil and Gas Authority, we have kept the incident reporting thresholds in line with the inclusion for OES thresholds, as well as aligning them with the existing BEIS voluntary reporting system for oil and gas supply disruptions.
- Thresholds for gas storage and LNG facilities have been aligned with the rest of the upstream sector, as we consider these facilities to have the same impact on security of supply.
- The threshold of 8,219 tonnes oil equivalent per day has been reached by dividing the annual threshold for inclusion in the NIS Regulations by 365 (3,000,000/365). This keeps both oil and gas thresholds aligned and aligns with the existing BEIS voluntary reporting system for production losses of 10 mcm per day of gas production.

Annex G - Incident Reporting Template

This form is not a regulatory requirement but is intended to be used by Operators of Essential Services (OES) to capture initial information on NIS incidents which should be sent to the relevant Competent Authority.

For Ofgem: cyberincident@ofgem.gov.uk

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

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.**

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

Points to capture	Response
Name of person reporting Role in the company Phone Email	
Name of the Organisation and the essential service it provides Internal incident ID number or name	
Date and time incident detected 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
- Description of the incident
- How the incident was discovered
- Duration
- Location 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

What investigations and/or mitigations have you or a third party performed or plan to perform

---

Who else has been informed about this incident? (CSIRT, NCSC, NCA, other Member States etc.)

What are your planned next steps?

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

Annex H - Voluntary Incident Reporting Guidance and contacting BEIS and NCSC

- BEIS undertakes voluntary collaboration work on energy cyber security, in partnership with the National Cyber Security Centre (NCSC) and wider energy resilience teams, 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 Critical National Infrastructure (CNI) operators regarding the reporting of cyber incidents.

You should 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 '**FOR ACTION**');

   OR

B. You assess is of wider interest (in communications this should be marked '**FOR INFORMATION**')

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

- Disrupt UK essential services or critical national infrastructure (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.

'**FOR INFORMATION**': 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:

1. You should be aware that the NCSC's Incident Management team are contactable on a 24/7 basis (on 0300 020 0973, or incidents@ncsc.gov.uk)

2. Please put in the header of any messages to NCSC whether your message is '**FOR ACTION**' or '**FOR INFORMATION**'. This will assist with triage and, when appropriate, help to expedite support from the NCSC.

3. 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.