Department for
Digital, Culture,
Media & Sport

Security of Network and Information Systems

Guidance for Competent Authorities

April 2018
Department for Digital, Culture, Media and Sport

Contents

About this Guidance

The goal of the Network and Information Systems Regulations of 2018 (NIS Regulations) is to drive improvement in the protection of the Network and Information Systems that are critical for the delivery of the UK's essential services.

This guidance gives information to Competent Authorities established under the NIS Regulations, and decision makers within those Competent Authorities, to help them:

- Establish an appropriate oversight and enforcement regime for the NIS Regulations;
- Assess the compliance by Operators of Essential Services (OESs) and Digital Service Providers (DSPs) in meeting the requirements of the NIS Regulations; and
- Develop a framework for national and international cooperation.

This Guidance:

- 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 Competent Authorities to make their own judgements or establish their own processes in accordance with the NIS Regulations.

1. Overview

The Security of Network and Information Systems Directive (known as the NIS Directive) provides legal measures to protect essential services and infrastructure by improving the security of their Network and Information Systems. The NIS Directive was adopted by the European Parliament on 6 July 2016. EU Member States have until 9 May 2018 to transpose the Directive into domestic legislation. The UK is implementing the requirements of the NIS Directive through a UK-wide set of Regulations - the Network and Information Systems Regulations 2018 (NIS Regulations), which will come into effect on 10 May 2018.

The NIS Regulation plays a key part in delivering the UK's National Cyber Security Strategy 2016-2021 and putting in place an effective regulatory framework to protect the UK's Critical National Infrastructure.

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. Member States will also need to participate in a CSIRT Network to promote swift and effective operational cooperation on specific network and information system security incidents and as well as the sharing of information about risks;

- Ensuring the framework for the security of network and information systems is applied effectively across sectors which are vital for our economy and society and which rely heavily on information networks, including the energy, transport, water, healthcare and digital infrastructure sectors. Businesses in these sectors that are identified by Member States as OESs will have to take appropriate and proportionate security measures to manage risks to their network and information systems. Operators of essential services will also be required to notify incidents to the relevant authority. Key DSPs - search engines, cloud computing services and online marketplaces - will also have to comply with the security and incident notification requirements established under the Directive.

On 23 June 2016, the EU referendum took place and the people of the United

Kingdom voted to leave the European Union. Until exit negotiations are concluded, the UK remains a full member of the European Union and all the rights and obligations of EU membership remain in force. During this period the Government will continue to negotiate, implement and apply EU legislation. The outcome of the negotiations on the future UK-EU partnership will determine what arrangements apply in relation to EU legislation once the United Kingdom has left the EU. It is the UK Government's intention that on exit from the European Union the policy provisions of the NIS Directive will continue to apply in the UK.

The UK held a public consultation from August to September 2017 on its proposals to implement the NIS Directive. This consultation covered six main topics:

- how to identify essential services;
- a national Framework to manage implementation;
- the security requirements for operators of essential services;
- the incident reporting requirements for operators of essential services;
- the requirements on Digital Service Providers; and
- the proposed penalty regime.

The Government received over 350 responses to its consultation. These responses showed that there was broad support for the Government's approach and that in the main, the Government's proposals were thought to be appropriate and proportionate.

The Government's response to the public consultation was published on 29 January 2018.

2. Oversight and enforcement

Oversight and enforcement of the NIS Regulations is the responsibility of the designated Competent Authority, and they will be held to account for their delivery of government policy within the National Framework. Although Competent Authorities are given duties and powers under the NIS Regulations for their sectors, the Department for Digital, Culture, Media & Sport (DCMS) has the role of oversight of implementation of the regulations across the UK.

The UK Government has decided that a multiple Competent Authorities approach, with each competent authority having a detailed understanding of the individual sectors and their associated challenges is the most appropriate approach for the UK. Competent Authorities have therefore been designated for each sector or region covered by the NIS Regulations. Their designation is set out in Schedule 1 of the Regulations.

Competent Authorities have the sole authority and responsibility for all regulatory decisions in relation to the NIS regulations. Competent Authorities will be supported by the National Cyber Security Centre (NCSC) who will offer technical advice to Competent Authorities, and who will carry out the duties of the SPOC and the CSIRT, except in the healthcare sector, in which cyber incidents will be handled by NHS Digital.

A list of Competent Authorities, broken down by sector can be found at Annex I.

2.1 Responsibilities of Competent Authorities

Competent Authorities are responsible for:

- reviewing the application of the NIS Regulations in their sector or region;
- preparing and publishing guidance to assist OESs or DSPs in meeting the requirements of the NIS Regulations;
- establishing the identification thresholds for the OESs in their sector or region;
- keeping a list of all OESs who are designated, including an indication of the importance of each operator;
- keeping a list of all revocations;
- consult and cooperate with each other, the CSIRT, SPOC and Information Commissioner's Office (ICO);
- assessing the compliance of operators to the requirements of the NIS Directive;
- determining the thresholds for reportable incidents in their sectors or region;

- cooperating with other Competent Authorities to provide consistent advice and oversight to OESs or DSPs;
- receiving incident reports;
- making sure that there are processes in place for non-cyber incidents and issuing guidance to support companies dealing with non-cyber incidents;
- incident investigation; and
- enforcement, including issuing notices and penalties, of the requirements of the NIS Regulations.

2.2 Monitoring the application of the NIS Regulations

OESs or DSPs, which meet the designation thresholds for that sector or have been designated by the reserve power, have the legal duty to comply with the requirements of the NIS Regulations.

Effective oversight will require a structured approach of engagement with designated operators. Competent Authorities should consider developing a oversight process by which they can monitor the application of the Regulations. The nature of this process is for the relevant Competent Authority to decide and to share with operators in its sector or region.

For Competent Authorities regulating OES, such a process must be proactive. This means that Competent Authorities for OESs should engage with industry, publish guidance, meet with representatives from OESs, and implement an assessment framework including an audit programme. An oversight regime that is not proactive, and that is based on active oversight only once an incident has happened would not be sufficient to meet the requirements of the NIS Regulations.

For the Information Commissioner's Office (ICO), responsible for regulating DSPs, the approach is limited to *post-ante* oversight (i.e post incident). The ICO, is therefore encouraged to provide guidance and support to DSPs and to have an effective means to spot when an incident has occurred and when they should take action.

2.3 Identification of Operators of Essential Services and Digital Service Providers

Essential Services

The thresholds to determine who is in scope of the NIS Regulations are set out in Schedule 2 to the Regulations. Different thresholds have been set for each sector: Water, Energy, Transport, Health, and Digital Infrastructure.

It is the responsibility of the OES to identify themselves and they should notify and engage with their relevant Competent Authority. However, Competent Authorities should be proactive in engaging with prospective OES in their sector or region.

If a Competent Authority believes that an entity is an OES and that entity has not engaged with the Competent Authority, the NIS Regulations contain powers to enable the Competent Authority to obtain the necessary information to determine whether they do meet the threshold requirements and to formally designate that entity as an OES.

If a Competent Authority believes that an entity that satisfies the thresholds should not be identified as an OES, the Competent Authority may revoke the deemed designation, by notice. Similarly, a competent authority may revoke a designation if the entity no longer met the conditions to be identified as an OES.

If an OES is not sure whether they are in scope of the NIS Directive, it is their responsibility to contact the relevant Competent Authority to receive that clarification.

If 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, the Competent Authority can make a determination to designate that entity as an OES in accordance with regulation 7 of the NIS Regulations. This designation power should only be used as an exception to bring in select OESs. The reasons for designating the organisation should be made clear to the entity, and where possible, designation should be agreed with that entity in advance to avoid unnecessary legal challenges.

Competent Authorities are required to maintain a list of OES for their sector or region, and liaise with Competent Authorities covering the same sector in devolved administrations, so that the UK can fulfil its national reporting obligations. The SPOC is in charge of forwarding an annual report containing the number and relevance to other Member States of OES to the European Commission. It is the responsibility of Competent Authorities to maintain a list of OES in their sector or region, and to update it on a biennial basis.

Digital Service Providers

Online Marketplaces, Search Engines, Cloud Service Providers are considered DSPs. The NIS Regulations contain further explanations of these definitions, as does the Government Response to the consultation.

DCMS considers that in order for a DSP to be in scope of NIS, they have to provide their services to external bodies or customers. For example, if an operator provides Domain Name System (DNS) services for its employees but not for customers, that operator will not be in scope. If an organisation is both an OES and a DSP, that organisation will be required to follow both regimes under the NIS Directive. In such circumstances, DCMS strongly advises the Competent Authority and the ICO to work together to reduce duplication of effort for themselves and the regulated operator, and to ensure that the operator does not experience inconsistency.

DSPs who are small or micro enterprises - those with fewer than 50 staff and/or a turnover of €10m a year) - are exempt from the requirements of the NIS Regulations. This exemption for small and micro businesses is intended to reduce the regulatory burden on small business, and only applies for individual firms. A firm that is part of a larger group may need to include staff headcount/turnover/balance sheet data from that group too. This is covered in Commission Recommendation 2003/361/EC, which is the reference for the SME carve-out at Article 16(11) of the NIS Directive.

DSPs are required to register with the ICO within a timeframe specified by the ICO. This registration is intended to facilitate the identification of DSPs. DCMS encourages the ICO to put such a registration process in place as soon as is practicable and inform DSPs, and potential DSPs, as necessary.

2.4 Determination of incidents

As set out in the NIS Regulations an incident is:

- Any event that has an actual adverse effect on the security of network or information systems used in the provision of essential services;
- where the security of network and information systems means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems; and
- that has a significant impact on the continuity of essential services they provide.

For OESs, it is the responsibility of the relevant designated Competent Authority in each sector to publish the incident reporting thresholds for each sector which determine the significant impact that will apply under NIS. Guidance on determining incident reporting thresholds was circulated to Competent Authorities in November 2017.

For DSPs, the incident reporting thresholds are set out in the Commission Implementing Regulation 2018/151 of 30 January 2018.

DCMS encourages Competent Authorities to discuss and seek the agreement of the relevant sectoral Lead Government Department (or devolved Government Department if the sector is devolved) and the NCSC, before any parameters are finalised or published. Competent authorities will need to inform the OES, and are expected to engage with industry when determining relevant parameters. Where a sector is partially devolved, Competent Authorities should coordinate with other Competent Authorities in that sector to agree common parameters.

In the case of Northern Ireland, cross-border engagement with the Republic of Ireland is also encouraged. The aim of this engagement is to align the approaches both North and South of the border to support the smooth operation of NIS services that cover both countries. Hence, Competent Authorities in Northern Ireland should engage with other Competent Authorities in the UK and Competent Authorities in the Republic of Ireland, keeping HMG and the SPOC informed of progress as necessary.

2.5 Enforcement

If an OES or DSP is not compliant with the NIS Regulation, Competent Authorities can take a number of actions to inform and enforce their decisions, through the use of Information Notices and Enforcement Notices. The process for this is set out in the NIS Regulations, which have been designed to give as much flexibility as possible to the Competent Authorities as to the exact process that any enforcement action takes.

In their approach to enforcement, Competent Authorities should note that simply having an incident is not by itself an infringement of the NIS Regulations, and that the key factor for determining enforcement action is whether or not appropriate and proportionate security measures and procedures were in place and being followed.

When establishing their enforcement processes, or undertaking enforcement action, Competent Authorities must be as transparent as possible. Transparency is one of the statutory principles of good regulation and underpins key provisions of the Regulators' Code or the Scottish Regulators' Strategic Code of Practice. It is essential that Competent Authorities publish their enforcement policy so that OESs and DSPs are clear as to the approach being taken. Competent Authorities should implement a stepped process of enforcement in which OES and DSPs are given warnings.

In considering an enforcement action, including financial penalties, Competent Authorities will need to ensure that this action is appropriate and proportionate, and must take the following mandatory factors into account:

- any representations made by the OES or DSP;
- any steps taken by an OES or a DSP towards complying with the requirements set out in the regulation;
- any steps taken by an OES or a DSP for remedying the consequences of any failure to comply;
- whether the OES or DSP has had sufficient time to implement the requirements of the Regulations; and
- whether the contravention is also liable to enforcement under another regulatory regime.

Competent Authorities should also note their requirements to comply with the Growth Duty, which requires that any person exercising a regulatory function must have regard to the desirability of promoting economic growth (the “growth duty”). In performing their duties, must consider the importance for the promotion of economic growth of exercising the regulatory function in a way which ensures that regulatory action is taken only when it is needed, and any action taken is proportionate.

There is risk of infringing more than one piece of legislation at a time, because operators will be required to comply with a wide range of legislation. If an infringement occurs that breaches more than one piece of legislation, Competent Authorities should have regard to this and where possible discuss the best approach with other regulators, but they will remain free to undertake their own response to any infringement, provided that it is appropriate and proportionate.

If the Competent Authority concludes that an OES or a DSP shall receive a financial penalty, the results of the investigation and the rationale for the financial penalty should be shared with the OES or DSP.

2.6 Monetary penalties

Competent Authorities have the authority to level substantial financial penalties if necessary, in line with the requirements of the NIS Regulation. In all consideration of penalties, Competent Authorities will be required to determine that the penalty be appropriate and proportionate to the contravention in respect of which it is imposed and the sectoral context. Competent Authorities will take into account representations from the operator, steps taken to comply with the NIS Regulations, actions taken to remedy any consequences, as well as other legislation that may have been breached.

Competent Authorities should provide consistency in approach across the whole of the UK and between sectors, within reason and taking into account considerations for each sector or region. What's a reasonable and proportionate monetary penalty will vary depending on the sector. Competent Authorities should implement a penalty framework that is robust, proportionate, transparent and defendable. The criteria in this penalty framework should be well defined and unambiguous.

2.7 Appeals

In line with the Regulators' Code and the Scottish Regulators' Strategic Code of Practice, Competent Authorities are required to provide an impartial and clearly explained route to appeal against regulatory decisions or a failure to act in accordance with the Regulators Code. This can be an internal process, but individual officers of the regulator who took the decision or action against which the appeal is being made should not be involved in considering the appeal.

In addition, the NIS Regulations require Competent Authorities to establish - when requested - an independent appeals process for appeals against:
designation of OES who do not meet the thresholds; and
any monetary penalties.

This appeals process is intended to supplement a Competent Authorities existing appeals process. Competent Authorities should ensure that their appeal processes, whether independent or internal, are fair, transparent, and publicised to those who are regulated.

2.8 Cost recovery

For the purposes of carrying out an audit or inspection, the OES or DSP can be asked to pay the reasonable costs of the inspection. The NIS Regulation also includes a power to permit Competent Authorities to recoup reasonable costs from those that they regulate.

A Competent Authority can establish a regime to recoup reasonable costs incurred by, or on behalf of, that Competent Authority in carrying out a relevant function under the NIS Regulations (see Part 6 of the Regulations). The Competent Authority must submit an invoice to the OES or DSP stating the work done, the reasonable costs, and the time period to which the invoice relates. The fee must be paid by the OES or DSP within 30 days after receipt of the invoice, and it is recoverable as a civil debt.

If a Competent Authority wishes to recoup costs through a fixed fees based regime, the Competent Authority may need to establish a new fee regime for this purpose.

As with any new fee regime, Competent Authorities should seek approval from their respective Government departments and/or HM Treasury before introducing any fee. Any fee regime should be transparent, and take into account the impact on the sector (for example by consultation with the sector). If such a regime requires additional legislation to implement, the Competent Authority should agree this with their relevant Government department.

3. Assessing compliance

3.1 Security Measures

Essential Services (OES)

Competent Authorities are required to assess the compliance of OES with the requirements of the NIS Regulations. Compliance should be assessed against the 14 principles laid out in the NIS Consultation and the associated security guidance published on the NCSC's website.

The security principles and associated security guidance carry no assumptions about how the required outcomes should be achieved, including risk management. It is for the OES to determine the most appropriate security measures within their organisational context in discussion with the relevant Competent Authority to deliver these outcomes. Competent Authorities should advise on these measures and give directions on how to achieve them.

The NCSC will publish a Cyber Assessment Framework (CAF), which is designed to provide a common framework for Competent Authorities to assess compliance against these security principles and guidance.

Although it is not compulsory, Competent Authorities are strongly encouraged to use the CAF in order to provide consistency across sectors and the UK as a whole. If a Competent Authority does not use the CAF, then it will need to set out its own assessment framework, which will need to provide an equal level of assurance, and show how this alternative assessment framework maps to the CAF. It should take advice on the equivalence of such frameworks from the NCSC as the UK's National Technical Authority.

DCMS recommends that Competent Authorities consider instructing OES to assess themselves against the CAF and submit their findings to their relevant Competent Authority, if required, supported by independent assurance from a third party approved by the Competent Authority or NCSC. Where deficiencies are identified, this should be accompanied by an action plan detailing how and when these deficiencies will be addressed. Competent Authorities could use the results of this self-assessment to drive their proactive engagement, audit programme and further guidance. Competent Authorities are not obliged to follow the self-assessment approach and are able to conduct the assessment directly. Whatever the approach, Competent Authorities should ensure a common baseline across each sector and the UK as a whole.

Using the results of this initial assessment, Competent Authorities should work with OESs in their sectors to agree where and when improvements to network and information security should be made. In order to do so, Competent Authorities should seek relevant expertise and pursue a coherent and consistent approach. OESs will propose to their relevant Competent Authority what measures they consider are appropriate, but it is ultimately for the Competent Authority and not the OES to make a determination.

Competent Authorities should establish a process for the ongoing assessments of compliance with the security requirements of the NIS Regulations. DCMS encourages Competent Authorities to publish their process, setting out how they will monitor and assess compliance, the frequency of audits or inspections, and the process that they will follow to assess risk. Publishing such a process will ensure that the assessment process is transparent and that each OES knows what will be expected of them. The frequency and nature of audits or inspections is for Competent Authorities to establish, seeking consistency between sectors and across the UK, and being alert to the burdens and costs that audits or inspections can place on OES.

Competent Authorities are free to prioritise compliance with individual principles according to the needs of their sector and may place more emphasis on certain elements depending on sector priorities and risks. If necessary, Competent Authorities should issue sector specific guidance and monitor compliance with these in addition to the main NCSC guidance. The purpose of such sector specific guidance is to cover sector specific issues that the main guidance may not adequately cover. Initial sector specific guidance should, where possible, be published before November 2018.

Digital Service Providers (DSPs)

The broader security requirements for DSPs have been set at a European level, in order to provide consistency across the Single Market. The ICO will need to ensure that the guidance it produces in order to assist DSPs in meeting their obligations under the NIS Regulations is consistent with that produced by other EU Member States. DCMS recommends that the Competent Authority takes the guidance published by the European Network and Information Systems Agency (ENISA) for digital service providers as its starting point for its own guidance, as well as any subsequent guidance published by the NIS Cooperation Group.

Non Cyber measures

The aim of the NIS Regulations is to minimise the risk of disruption to services due to the failure of a key network or information system. Although the main focus of the

Regulations is to respond to the rising cybersecurity challenge, OESs and DSPs are also expected to identify and manage the risk of other potential causes of failure in a proportionate manner, this includes physical events that might have an adverse effect on Network and Information Systems.

The NCSC's 14 Security Principles and associated Security Guidance, and the measures set out for DSPs in the Commission's Implementing Regulation, are primarily focused on ensuring adequate cyber security risk management, but OESs and DSPs will also need to take into account broader resilience issues when considering the security of their network and information systems. Network and information systems supporting essential services should be resilient to wider risks such as loss of power supply, hardware or software failure, physical damage and environmental hazards. OES should also consider their capability for disaster recovery (i.e. offsite backup, re-location).

Competent Authorities should provide guidance to OESs and DSPs on the physical measures that they should consider. Competent Authorities should use their judgement on the appropriate measures required, using guidance provided by ISO, NIST Framework, the ENISA guidelines and other Government Departments.

NIS does not apply directly to the supply chains of OES and DSPs. However, the NCSC has produced guidance on supply chains as part of its overall NIS guidance, which should be taken account of. It is the OES or DSP's responsibility to ensure that their suppliers have in place appropriate measures, and that appropriate and proportionate measures are put in place to manage the risk of their services being disrupted via their supply chain.

3.2 Incident reporting

OES must report any incidents where the interruption or reduction in services exceeds the threshold value set for that OES, as determined by the relevant Competent Authority (see section 2.4). For DSPs, the incident reporting thresholds are set at a common level across Europe, as set out in the European Commission's Implementing Regulation.

All incident reports should be submitted to the relevant Competent Authority within 72 hours. The incident reports submitted to Competent Authorities have regulatory purposes. If an OES or a DSP requires incident response support, they need to contact the appropriate authorities as soon as the event has been detected. If the incident involve criminal matters, the affected OES or DSP should also involve the relevant law enforcement agency.

An event is considered to have an impact on a service if it disrupts or interferes with

the service itself. DCMS highlights that the source of such events is not be limited to network and information systems that directly operate an essential service. OES and DSPs should consider the impact of failure in other network and information systems, such as billing or payment services, and whether they could have an impact on the provision of an essential service. Competent Authorities will need to ensure that OESs are aware of the risk of service loss through their wider network and information systems and take steps to mitigate those risks.

For reportable incidents under NIS, DCMS recommends that Competent Authorities publish clear guidance to OESs and DSPs in their sector on how they should report an incident and what information needs to be reported. Competent Authorities should also consider guidance on the separate expectations on OESs and DSPs to report incidents to the NCSC, LGDs and other Government bodies to support incident response/management under voluntary frameworks.

The Competent Authority should maintain a log of all incidents and establish a process to use the incident reports to assess whether any subsequent investigation is required. This will be a standalone process and will not form any part of the incident response.

If an incident with an OES involves a loss of service to one or more other EU Member States, the Competent Authority should inform the CSIRT immediately so that the CSIRT can alert the other Member States. The Competent Authority should cooperate with the relevant authorities of the other Member State to the best of its ability, taking into account any data protection or commercial sensitivities that may be involved. For DSPs, the approach is different and the ICO should inform the SPOC of the other Member State directly.

Voluntary reports of incidents that do not meet the sectoral incident reporting thresholds can be submitted to either the Competent Authority or the NCSC. This should be actively encouraged. Organisations that are not designated as OESs or DSPs should also be encouraged to submit voluntary reports. Voluntary reports should be treated ‘in confidence’ and should not lead to regulatory action.

3.3 Incident response

When an OES or a DSP reports an incident, the Competent Authority has the responsibility to:

- make sure that OESs know they need to contact the NCSC directly for incident response support in the case of cyber incidents (or NHS Digital in the health sector);
- where appropriate, encourage the OES or DSP to use existing emergency structures for incident response support in the case of non-cyber incidents.

- inform the CSIRT if the incident has affected other Member States so that information can be shared; for DSPs, the ICO should inform Member States direct;
- monitor the incident as necessary;
- if appropriate, announce and disseminate information for relevant stakeholders, including other OESs, about the incident, including giving them incident warnings; and
- conduct incident investigations.

Competent Authorities should set out their expectations of OESs and DSPs in relation to management of incidents resulting from non-cyber events, such as hardware failure or environmental hazards. It is the responsibility of the OESs and DSPs to manage their incidents and to ensure that they are receiving the support they need.

If an incident occurs that couldn't be avoided through compliance with CAF or guidance issued by the Competent Authority, the Competent Authority has the flexibility to manage its response in a way that best suits the incident and the resources available (i.e does not have to take action). In doing so, the Competent Authority should take into account that it is not possible for OESs and DSPs to account for or mitigate every possible risk.

3.4 Incident investigation

Competent Authorities are free to decide when an incident requires further investigation. There is no requirement to investigate every incident and Competent Authorities are recommended to establish some form of triage system to classify incidents in terms of importance.

The purpose of this investigation is to:

- assess whether the incident was preventable;
- assess whether effective and reasonable risk management was in place;
- assess whether the operator had appropriate security measures in place; and
- assess how the OES responded to and managed the incident.

Once the investigation has concluded, it is up to the Competent Authority to decide on the next appropriate step, be it advice, enforcement action, penalties or no action, and in accordance with its own procedures and published enforcement policy..

The ICO, on behalf of DCMS, is preparing a proposed NIS incident investigation manual. This manual will include detailed information on how to identify an incident,

how to gather evidence and assessment on the impact of the incident. The objective is to create a dynamic process with fast track actions to advance the investigation. The ICO investigation manual will be supported by guidance provided by the NCSC. This manual will not be obligatory and is not intended to replace existing investigation frameworks. It is primarily intended to support those Competent Authorities who do not have an existing investigation framework.

All Competent Authorities should share the results of any investigation with the concerned OES or DSP, both for reasons of transparency and fairness, and because an OES or DSP can find this information useful to improve the resilience of their systems.

4. Develop a framework for national and international cooperation

Collaboration is an essential to ensure effective oversight of NIS in the UK. In order for the NIS Directive to be implemented successfully, Competent Authorities are encouraged to proactively engage with industry, and work closely with other organisations, the devolved administrations and each other. Competent Authorities should work closely with the devolved administrations and each other and, where possible, have an agreement to interact with other Competent Authorities when an incident originating from one part of the UK has an impact on another part of the UK with different regulators, or an incident impacting multiple parts of the UK.

4.1 National Cooperation

DCMS has been chairing a regular meeting of Competent Authorities in order to coordinate and support Competent Authorities in their preparations for the coming into force of the NIS Regulations. It is DCMS's intention to continue to host such meetings after the Regulations come into force in order to provide a forum for Competent Authorities to share their expertise and experience, and to encourage close cooperation at a working level. DCMS strongly encourages Competent Authorities to continue to participate. Over time, it is DCMS's intention that this forum will become the main forum for Competent Authorities to share information and to cooperate with each other.

4.2 Computer Security Incident Response Team (CSIRT)

The NCSC will be the Computer Security Incident Response Team (CSIRT) under the NIS Regulations. The CSIRT's role is to provide incident support and assistance to OESs and DSPs on cyber matters, and their support is available 24/7. The CSIRT will monitor security incidents at national level; provide early warning, alerts, announcements and dissemination of information to relevant stakeholders about threats, risks and security incidents; respond to security incidents; provide dynamic risk and incident analysis and situational awareness. However, NCSC is not a substitute for the incident management function in an OES or a DSP and the level of assistance they will provide depends on the impact and cause of the incident.

The CSIRT will not receive incident notifications directly, and, as previously stated, Competent Authorities are encouraged to recommend that OESs and DSPs contact the CSIRT directly for support in the event of a cyber-incident. Competent Authorities should provide guidance to OESs and DSPs that clarifies that, if they need cyber-

incident support, they need to contract the CSIRT directly (or NHS Digital in the health sector), and, preferably as soon as the incident has been detected. OESs and DSPs can then submit their mandatory report to their relevant Competent Authority within 72 hours of the incident being detected.

Competent Authorities for OESs must inform the CSIRT about any incident that may have a cross border impact. The CSIRT will then inform the other affected Member State. Cross border in this case refers to international borders only.

For DSPs, the ICO should contact the relevant SPOC in the other affected Member State~~s~~ directly.

The NCSC, in its role as national technical authority for cyber security, will also work closely with Competent Authorities providing expertise and advice and by facilitating the exchange of best practice.

4.3 Single Point of Contact (SPOC)

The NCSC will also act as the single point of contact under the NIS Regulations. The SPOC's role is primarily a liaison role, facilitating cross-border cooperation and communication. The SPOC will submit annual reports to the Cooperation Group containing the number of incidents and the nature of these incidents. The first one of these reports will be submitted on 9th August 2018, and Competent Authorities are required to provide this information by 9th July. The SPOC will also submit biennial reports identifying the number of OESs for each subsector. The first on of these reports will be submitted on 9th November.

4.4 Other Competent Authorities

Competent Authorities are encouraged to cooperate with one another, and where possible to have common procedures. However, DCMS recognises that there will sometimes be a need for divergence between sectors and regions. This arises in particular where there are differences within the devolved administrations and procedures may differ. Competent Authorities have the flexibility to adapt their approach to reflect the needs of their sector or region.

Where there are OESs that provide essential services to more than one sector or region, or also qualify as a DSP, 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.

4.5 Other regulators

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

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

4.6 The Government

Regulatory responsibility for enforcing the NIS Regulations lies solely with Competent Authorities. However, the departments of the UK Government and the devolved administrations are also involved and have responsibilities for matters that can directly affect both Competent Authorities, their sectors and Operators within them. The UK Government also has responsibility for national security. Competent Authorities are therefore strongly encouraged to engage and maintain a close relationship with the relevant UK departments and the devolved administrations, where the Competent Authority is not a government department. The UK Government will continue to liaise closely with the devolved administrations.

4.7 The Cooperation Group

The NIS Cooperation Group was established to support and facilitate strategic cooperation between Member States regarding the security of network and information systems. The Cooperation Group is composed of representatives of Member States, the Commission, and the ENISA.

The Cooperation Group:

- discusses the capabilities and preparedness of the Member States;
- examines, on an annual basis, the summary reports from each Member State;
- assesses the implementation of the NIS Directive in each Member State every two years;
- establishes a work programme, every two years, in respect of actions to be undertaken to implement the objectives and tasks of the NIS Directive;
- periodically reviews the NIS Directive, with a view to determine the need of modification in the light of societal, political, technological and market changes;

- receives notifications on the designation of Competent Authorities and single point of contact, their tasks, and any subsequent change thereto; and
- exchanges best practice on the exchange of information related to incident notification, and discuss modalities for reporting notifications of incidents.

DCMS is the UK representative. DCMS will represent the interests of UK Competent Authorities, the CSIRT and the SPOC; and share any guidance produced by the Cooperation Group. Competent Authorities should interact with the Cooperation Group through DCMS.

5. Timeline

There are a number of events that are required to take place at a certain time under the NIS Regulations. The timeline for these events is as follows:
:

- May 2018: NIS legislation comes into effect. OESs that meet the identification thresholds come into scope automatically;
- July 2018 (and each year after): Annual report of NIS incidents submitted to the SPOC, for them to submit to the European Commission in August 2018 and every year thereafter;
- November 2018: Sector specific guidance published as necessary in line with commitments made in the public consultation;
- November 2018 (and biennially after): Report of number of OESs and the thresholds for identification submitted to the EU by the SPOC; and
- May 2019: Annual review of the regulatory provisions of the NIS Regulations.

5.1 First year

OESs vary in the current level of maturity and existing sectoral security and resilience requirements. In some sectors it will be difficult for OESs and DSPs to demonstrate that they are fully compliant with the requirements of the NIS Regulations by May 2018. Competent Authorities should have reasonable expectations and expect some OESs not to be fully compliant by May 2018, given that the NIS Regulations will be published in early April 2018. DCMS recommends that Competent Authorities take an approach which gives OESs and DSPs enough time to reach the appropriate levels of security requirements, and is proportionate to the risk of significant impact on an essential service.

DCMS proposes that the main priority for Competent Authorities in the first year should be to obtain a clear picture of the security of network and information systems in their sectors. OESs should be expected to begin analysing their systems and existing security measures in order to understand where further work needs to be done, and to develop plans in order to reach the appropriate levels of security requirements. Competent Authorities have the responsibility to issue clear guidance to their respective OESs on applicable benchmarks against which to assess their systems.

Given the challenges facing OESs and DSPs, DCMS recommends that Competent Authorities take a cautious approach to enforcement during the first year. This does not mean that a Competent Authority cannot consider penalties during the first year of implementation - if an OES or a DSP is considered to be seriously negligent in the implementation of security measures or the handling, or reporting of an incident, that OES or DSP may receive a penalty notice. However, as enforcement has to be

proportionate and appropriate, DCMS recommends that Competent Authorities take into account the challenges arising for OESs and DSPs from a lack of comprehensive NIS compliance guidance prior to May 2018.

5.2 EU exit implications

At this stage, it not possible to be wholly certain of the outcome of negotiations of the UK's exit from the EU. The outcome of the negotiations on the future UK-EU partnership will determine what arrangements apply in relation to EU legislation once the United Kingdom has left the EU. However, the Government has made clear that it intends to maintain the NIS Regulations post EU exit. DCMS will keep Competent Authorities and devolved administrations fully informed of any changes, including:

- how the provisions can continue to apply post exit;
- how the UK will engage with institutions established pursuant to the NIS Directive; and
- the impact on Competent Authorities regulating OESs with a cross-border reach, paying special attention to the border between Ireland and Northern Ireland.

Regardless of the UK's participation in the EU it is clear that if an OES or a DSP operates in the UK, they will have to comply with UK legislation, and that if they want to operate in the EU, they will have to comply with EU legislation and with the legislation of the EU country where they want to operate.

Annex I: List of Competent Authorities

Sector: Drinking water supply and distribution

Subsector: n/a

Competent Authority:

In England, the Secretary of State for Environment, Food and Rural Affairs.

In Wales, Welsh Ministers.

In Scotland, the Drinking Water Quality Regulator.

In Northern Ireland, the Department of Finance.

Sector: Energy

Subsector: Electricity

Competent Authority:

In England, Scotland and Wales, the Secretary of State for Business, Energy and Industrial Strategy and the Office of Gas and Electricity Markets (Ofgem). (Joint Competent Authorities)

In Northern Ireland, the Department of Finance.

Subsector: Gas

Competent Authority:

In England, Scotland and Wales, for natural gas undertakings that carry out the function of production, operators of natural gas refining and treatment facilities, storage system operators and LNG system operators, the Secretary of State for Business, Energy and Industrial Strategy. Otherwise, the Secretary of State for Business, Energy and Industrial Strategy and the Gas and Electricity Markets Authority, acting jointly

In Northern Ireland, the Department of Finance.

Subsector: Oil

Competent Authority:

In England, Scotland and Wales, the Secretary of State for Business, Energy and Industrial Strategy.

In Northern Ireland, the Department of Finance.

Sector: Digital Infrastructure

Subsector: n/a

Competent Authority: The Office of Communications (Ofcom)

Sector: Health Sector

Subsector: Health care settings

Competent Authority:

In England, the Secretary of State for Health.

In Wales, Welsh Ministers.

In Scotland, Scottish Ministers
In Northern Ireland, the Department of Finance.

Sector: Transport

Subsector: Air transport

Competent Authority:

The Secretary of State for Transport and the Civil Aviation Authority.

Subsector: Maritime transport

Competent Authority:

The Secretary of State for Transport.

Subsector: Road transport

Competent Authority:

In England and Wales the Secretary of State for Transport.
In Scotland, Scottish Ministers.
In Northern Ireland, the Department of Finance.

Subsector: Rail transport

Competent Authority:

In England, Scotland and Wales the Secretary of State for Transport.
In Northern Ireland, the Department of Finance.

Sector: Digital Service Providers

Subsector: Cloud Services; online marketplaces; Search engines;

Competent Authority:

The Information Commissioner's Office (ICO).

References

Security of Network and Information Systems Directive: link here

Consultation on the Security of Network and Information Systems Directive: link here

Analysis of responses to public consultation: link here

Government response to public consultation: link here

NCSC NIS Guidance Collection: link here

Commission Implementing Regulation (EU) 2018/151 of 30 January 2018: link here

The Regulators Code (2014): link here

The Scottish Regulators' Strategic Code of Practice: link here

The Growth Duty (2017): link here