GUIDANCE ON THE IMPLEMENTATION OF THE NETWORK AND INFORMATION SYSTEMS (NIS) REGULATIONS 2018

DAY 1 GUIDANCE

DOCUMENT CONTROL
The only controlled version of this document can be accessed on the DWI Website

Printed copies of this document, together with electronic copies held on local computers and other storage devices are uncontrolled.

CONTENTS

1. INTRODUCTION AND PURPOSE

1.1 The purpose of this Day 1 Guidance is to provide an overview of the implementation of the Network and Information Systems (NIS) Regulations 2018 for the water sector and inform operators of the essential service (OES) of what to expect when the Regulations come into effect on 10 May 2018.

1.2 There is particular focus on the incident reporting thresholds, the process to notify a NIS incident and incident support.

1.3 This Guidance has been issued by the Drinking Water Inspectorate (DWI), who undertake the operational responsibilities of the competent authority function, for the sector on behalf of the Secretary of State and the Welsh Ministers, and in compliance with regulation 3 of the NIS Regulations 2018.

1.4 Further Guidance documents will be issued over the course of the first year which will focus on specific sections of the NIS Regulations and where deemed necessary.

2. THE NIS REGULATIONS

2.1 The Security of Network and Information Systems (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 and 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 the NIS Regulations 2018, which come into effect on 10 May 2018.

2.2 The NIS Directive specifies the types of entities that all Member States should consider for inclusion (Annex II of the Directive). In the UK, designation of organisations as OES will be achieved through setting thresholds in legislation relating to the scale of an organisation's operations. 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.

3. IMPLEMENTATION OF THE NIS REGULATIONS WITHIN THE WATER SECTOR

3.1 Drinking water supply and distribution has been designated an essential service within Schedule 1 of the Regulations.

3.2 The threshold requirement for an OES within the water sector is identified in Schedule 2 of the Regulations as the supplier of potable water to 200,000 or more people. Water companies that meet this threshold will automatically be designated an OES when the Regulations come into effect.

4. DESIGNATED COMPETENT AUTHORITY

4.1 Oversight and enforcement of the NIS Regulations is the responsibility of the designated Competent Authority (CA). CA's have the sole authority and responsibility for all regulatory decisions in relation to the NIS Regulations.

4.2 The National Cyber Security Centre (NCSC) will offer technical support to CA's and OES through their NIS Guidance Collection. Under the Regulations the NCSC will also undertake the duties of the Single Point of Contact (SPOC) and the Computer Security Incident Response Team (CSIRT).

4.3 For the water sector in England, the Secretary of State is the designated competent authority. Operational responsibilities of the competent authority function under the Regulations have been conferred to the DWI who will act on behalf of the Secretary of State under Section 86(1)(b) of the Water Industry Act 1991 (the 1991 Act), as amended.

4.4 In Wales, the Welsh Government is the designated competent authority. Operational responsibilities of the competent authority function under the Regulations have been conferred to the DWI who will act on behalf of the Welsh Ministers under Section 86(1)(b) of the 1991 Act, as amended.

5. NIS INCIDENT REPORTING THRESHOLDS FOR THE WATER SECTOR

5.1 There is a duty, set out in regulation 11(1) of the Regulations, for an OES to notify the CA of an incident that has affected the network and information systems (a NIS Incident), which has had a significant impact on the continuity of the essential service.

5.2 A 'significant impact on the continuity of the essential service' is one that meets any of the following thresholds:

- Any occurrence, apprehended or otherwise of where the company has identified any interference with electronic systems that has impacted on the supply, quality or sufficiency of water.

- Any loss of an Operational Technology (OT) systems that has impacted on the supply, quality or sufficiency of water.

- Any loss of Information Technology (IT) systems that has impacted on the supply, quality or sufficiency of water.

5.3 A NIS reportable incident can be a cyber incident or a broader physical or resilience incident. Initial examples of NIS incidents are outlined in Annex 1a; this list is not exhausted and DWI will work with the sector to develop further incident examples that fall within these thresholds.

6. FURTHER REPORTING REQUIREMENTS

6.1 DWI will notify the Secretary of State and/or the Welsh Government of any incident that is notified under the NIS Regulations. DWI will also notify other Devolved Administrations if an incident has the potential to significantly impact on the continuity of the essential service within that Devolved Administration.

6.2 DWI also has a duty under regulation (11)(5)(b) to share the information provided by the OES during a NIS incident with the CSIRT as soon as reasonably practicable.

6.3 If, after notification to the CSIRT, the incident has the potential to significantly impact on the continuity of the essential service of other Member States then the CSIRT will inform the relevant authorities in that Member State. However the CSIRT is not required to inform other Member States in this way if the information submitted is deemed confidential by the OES and/or prejudice the security or commercial interests of the OES.

6.4 After receipt of the notification, DWI and/or the CSIRT will inform the public about the NIS incident if it is of the view that public awareness is necessary in order to handle that incident or prevent a future incident. In this instance the DWI and/or the CSIRT will consult each other, and the OES who provided the notification, before making a final decision to undertake this action.

6.5 DWI will provide a report to the SPOC outlining the number and nature of NIS incidents notified on an annual basis. The first report will be submitted on the 1 July 2018.

7. VOLUNTARY REPORTING AND INCIDENT RESPONSE FOR CYBER INCIDENTS

7.1 The NCSC is the national technical authority for cyber related incidents. To ensure the NCSC can fulfil its function as the UK's CSIRT and SPOC under the Regulations, OES should provide voluntary notification to NCSC of any cyber-security incident, even if the incident falls below or hasn't met the NIS thresholds outlined in Section 5.

7.2 DWI recommends that OES should not wait until an incident reaches the 'significant impact' threshold before seeking support from the NCSC and other parts of Government in containing and mitigating incidents that could risk affecting essential services.

7.3 Notifying DWI of incidents that have not met the incident reporting thresholds outlined in Section 5 is also actively encouraged. These notifications will be treated as Information Reports and the examples of the type of Information Reports which should be submitted are outlined in Annex 1b

7.4 OES will not be penalised for submitting an Information Report to DWI but these reports will assist in building up the level of activity within the sector.

7.5 For any cyber related incident notified to NCSC, the OES should follow the NCSC Notification Guidance, outlined in Annex 2.

8. INCIDENT SUPPORT FOR NON CYBER INCIDENTS

8.1 The Secretary of State and/or the Welsh Government will provide support through their existing contingency structures for non-cyber incidents and broader resilience incidents.

9. NIS REPORTING PROCESS TO THE COMPETENT AUTHORITY

9.1 Notification of a NIS incident should be made without undue delay and unless it is not feasible, no later than 72 hours after the OES is aware that a NIS incident has occurred. Annex 3 outlines the reporting process for both NIS incidents and voluntary reporting to NCSC.

9.2 It is recognised that the person making the initial notification may not have all the required information to hand. It is also recognised that some of the information, as listed, may not be applicable to every incident.

9.3 OES should use the following procedure to notify a NIS incident:

1. Contact the Inspectorate via telephone, following the order specified in the cascade system (Annex 4)
2. Submit a completed Initial Report (Annex 5), which should be sent via email to dwi.NIS@defra.gsi.gov.uk.
3. The Inspectorate will acknowledge receipt of this email.

9.4 Notification of Information Reports will require a completed Initial Report to be sent via email to dwi.NIS@defra.gsi.gov.uk. The Inspectorate will acknowledge receipt of this email.

10. COMPLETING THE INITIAL REPORT

10.1 Examples of the type of information OES should include in their Initial Report is outlined below:

Detail	Required Information in Email
Incident Type	Reportable Incident/Information Report
Company Name	Company Name
The date and time the incident occurred	Date and Time of incident
The duration of the incident	Duration or estimate of duration (hours/days)
Description of Incident	Cyber/non cyber/resilience
Type of Incident	Denial of Service, Unauthorised Use/Access, Malicious Code, Internal issue, Power loss, Other
Information concerning the nature and impact of the incident	What systems has it impacted, Will customers be affected Impact within company, Back-up systems affected
Information concerning any, or any likely, cross-border impact of the incident	Company only, Sector only, Wider impact
Initial response by company to mitigate incident	Outline initial mitigation measures
Media interest	Yes/No
Other Agencies notified	Please specify e.g. NCSC, police
Has this triggered a Water Quality event notification	Yes/No
Any other information about the incident that the supplier considers relevant	Relevant Information

11. ASSESSMENT OF NIS INCIDENTS AFTER THE INITIAL NOTIFICATION

11.1 Following the Initial Notification, the DWI will decide whether or not the incident requires further investigation. The purpose of these investigations could be to: i) establish the cause of the incident and assess whether the incident was preventable; ii) assess whether effective and reasonable risk management was in place; iii) assess whether the operator had appropriate security measures in place; and iv) assess how the OES responded to and managed the incident.

11.2 The DWI will inform the OES whether follow-up investigations are required after receipt of the Initial Notification. If this is the case then an Interim Report should be submitted within 20 working days of this notification.

11.3 Once the investigation has concluded, the DWI will decide on any appropriate next steps, be it no action, advice or formal enforcement action.

12. EVENT NOTIFICATIONS UNDER THE WATER SUPPLY (WATER QUALITY) REGULATIONS 2016 OR THE WATER SUPPLY (WATER QUALITY) REGULATIONS 2018 (WALES)

12.1 Water companies already notify DWI of any event which, by its nature has, or is likely to adversely affect the quality or sufficiency of the water supplied. This requirement is set out in paragraph 9(1) of the Water Industry (Suppliers' Information) Direction 2017.

12.2 DWI expects that in most cases a reportable incident under the NIS Regulations will also be notified under the requirement outlined in Section 12.1.

12.3 Both the NIS incident and Water Quality event will be assessed separately and information around actions taken, mitigation required and whether any further action is needed will be outlined in individual assessment letters focusing on the respective regulations.

12.4 DWI expects that companies should have a clear understanding of when each notification is required and that clear communication channels are set up internally so that the relevant information is included in the respective reporting requirements to ensure compliance with both sets of Regulations

13. EXPECTATIONS WITHIN THE FIRST YEAR

13.1 The NCSC has developed the Cyber Assessment Framework (CAF) which is a tool that provides a systematic method for assessing the extent to which OES are achieving the outcomes specified by the NIS principles.

13.2 The CAF will provide statements of good and bad practice against each element of the security principles in order to be able to assess the maturity of an OES against that particular element.

13.3 An initial version of the CAF is now available however DWI plans to visit a selection of OES to test and validate the CAF in order to build up a specific profile for the sector. It is estimated that this will take 3-4 months. Once this testing and validation period has been completed then all OES will be expected to complete the CAF and submit this information to DWI. It is expected this self-assessment process will take a number of months for OES to complete and achievable deadlines will be set.

13.4 Over this period the OES will be expected to engage directly with the DWI, and to raise any queries they have on how to apply the assessment. Upon completion of the self-assessment, the DWI will work with OES to establish if and when improvements should be made. OES will need to propose what measures they consider appropriate and it will be for the DWI to determine whether they are sufficient.

13.5 Beyond the first year, the DWI will use the results of the self-assessment, along with threat and vulnerability information, to establish a risk-based programme of ongoing inspections to monitor compliance. Action will be focussed on OES where the most serious concerns have been identified and/or where potential incidents could have the greatest impacts on the sector.

13.6 DWI will issue further NIS Guidance documents on NIS Roles and Responsibilities, Incident Reporting, Inspections, Enforcement, and Response to Non-Cyber Incidents over the course of the year, with a completed set of Guidance Documents available by Nov 2018. These will all be made available through the DWI’s Website.

Annex 1: Notification Examples

a. Reportable NIS Notifications

The following occurrences are examples of reportable incidents that would meet the thresholds outlined in Section 5. This list is not exhaustive and OES are encourage to enter discussions with DWI if they are unsure whether an incident has breached the thresholds.

- Where the company have discovered interference by an external source (individual, state actor etc.) or an internal source (company employee)

- Loss of OT system which has resulted in a breach of the Water Supply (Water Quality) Regulations 2016 (England) or the Water Supply (Water Quality) Regulations 2018 (Wales)

- Loss of an OT system which has resulted in the non-availability of monitoring data to one or more sites

- Any business resilience issue that has impacted on the continuity of drinking water supply

b. Information Report Notifications

Relevant information reporting to the CA is actively encouraged and will assist in building up the level of activity within the sector. OES should submit an Information Report to DWI if the incident falls within one of the examples below.

- Any IT/OT issue that could have an effect on the supply, quality or sufficiency of the water supplied where the cause is unidentified

- The company have identified interference (external, internal or otherwise) within any IT/OT or physical security assets (including, if applicable, waste water assets) but there was no impact on the essential service

- The identification of unauthorised access within an OT system that the company deem to be suspicious

Annex 2: Incident Reporting to NCSC

To ensure the NCSC can fulfil its function as the UK's CSIRT and SPOC under NIS, and provide support with incident response, OES should provide notification of a NIS cyber-security incident to the NCSC at the earliest opportunity. This will ensure that the NCSC can, if necessary, respond promptly to help mitigate a serious incident, provide technical guidance, issue advice, and provide cross-Government co-ordination of the response. OES should also provide notification of cyber-security incidents to the NCSC that fall below or haven't reached the NIS thresholds. OES should use the following instructions as a guide.

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.

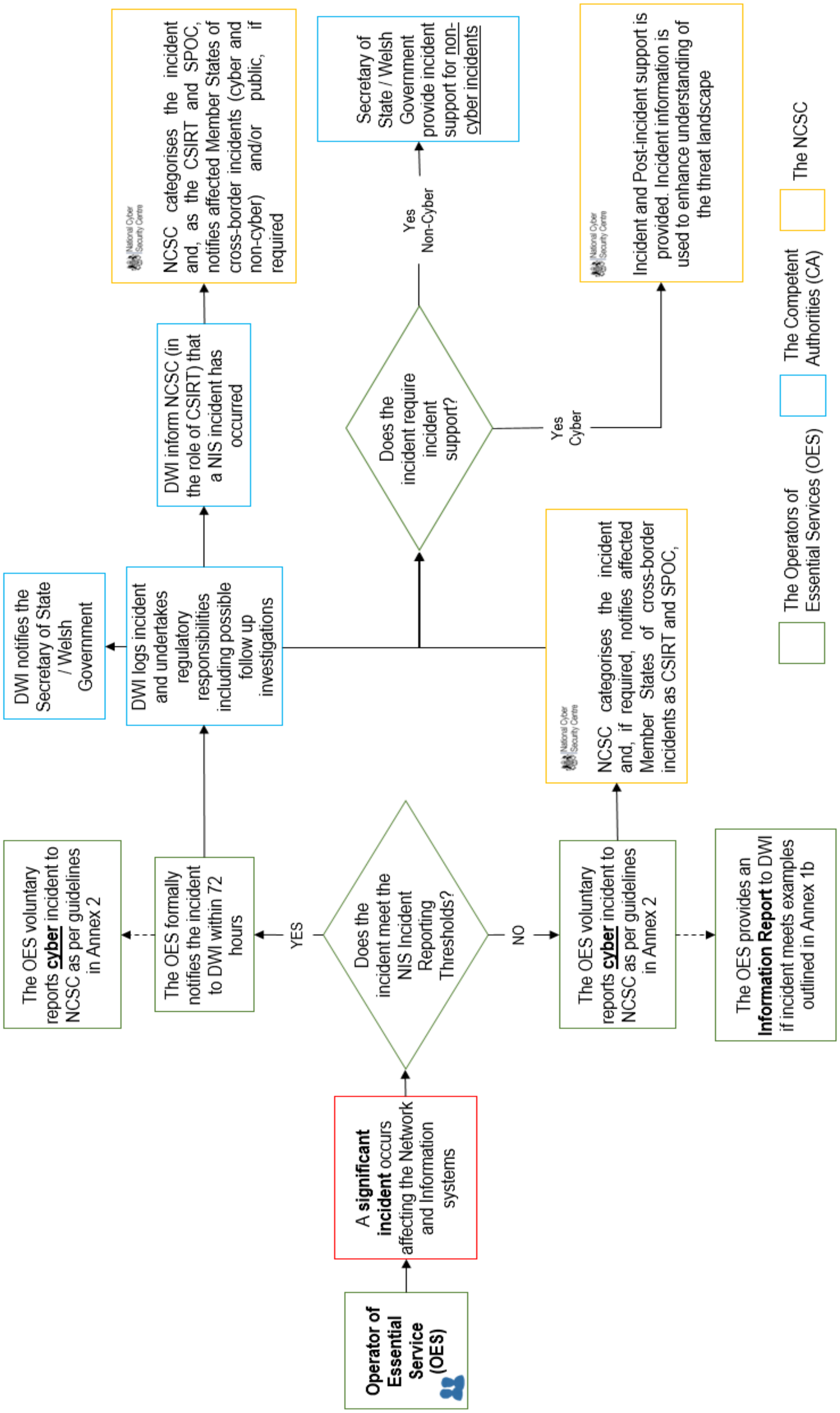
When contacting the NCSC:

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.

Annex 3: Reporting Flowchart



Operator of Essential Service (OES)
A significant incident occurs affecting the Network and Information systems
Does the incident meet the NIS Incident Reporting Thresholds?
YES
NO
The OES voluntary reports cyber incident to NCSC as per guidelines in Annex 2
The OES formally notifies the incident to DWI within 72 hours
The OES voluntary reports cyber incident to NCSC as per guidelines in Annex 2
The OES provides an Information Report to DWI if incident meets examples outlined in Annex 1b
DWI logs incident and undertakes regulatory responsibilities including possible follow up investigations
DWI notifies the Secretary of State / Welsh Government
NCSC categorises the incident and, if required, notifies affected Member States of cross-border incidents as CSIRT and SPOC,
DWI inform NCSC (in the role of CSIRT) that a NIS incident has occurred
NCSC categorises the incident and, as the CSIRT and SPOC, notifies affected Member States of cross-border incidents (cyber and non-cyber) and/or public, if required
Does the incident require incident support?
Yes Non-Cyber
Yes Cyber
Secretary of State / Welsh Government provide incident support for non-cyber incidents
Incident and Post-incident support is provided. Incident information is used to enhance understanding of the threat landscape
National Cyber Security Centre
The Operators of Essential Services (OES)
The Competent Authorities (CA)
The NCSC

Annex 4: Day 1 Call Cascade for NIS Notifications

Name	Contact Number
Steve Youell	07880 473237
Simon Benton	07909 007356
Mike Turrell	07909 007248
Laura Moss	07747 455889

Annex 5: Initial Report

NIS Initial Report: Required Information	
Incident Type	
Company Name	
The date and time the incident occurred	
The duration (or estimated) of the incident	
Description of Incident	
Type of Incident	
Information concerning the nature and impact of the incident	
Information concerning any, or any likely, cross-border impact of the incident	
Initial response by company to mitigate incident	
Media interest	
Other Agencies notified	
Has this triggered a Water Quality event notification	
Any other information about the incident that the supplier considers relevant	