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

ROLES AND RESPONSIBILITIES UNDER THE NIS REGULATIONS

CONTENTS

1. INTRODUCTION AND PURPOSE

1.1 The purpose of this Guidance Document is to provide an overview of the Network and Information Systems (NIS) Regulations and outline the roles and responsibilities within the water sector in order to deliver these Regulations

1.2 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 for Environment, Food and Rural Affairs and Welsh Ministers, and in compliance with regulation 3 of the NIS Regulations 2018.

1.3 Further Guidance Documents are available on the DWI website on the following topics:

- Incident Reporting Requirements
- The Cyber Assessment Framework (CAF)
- Inspections (Audits)
- Enforcement

1.4 These Guidance Documents will be amended as required to ensure they remain accurate and up to date. Additional guidance may be added to these documents if necessary or within another individual document if required.

2. OVERVIEW OF THE NIS REGULATIONS 2018

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 Network and Information Systems. The aims of the Directive are:

- 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 national Single Point of Contact (SPOC) for other Member States and a NIS Competent Authority (or Authorities);

- Setting up a Cooperation Group and a CSIRT Network; the former to facilitate strategic cooperation and the exchange of information among Member States and the latter to promote swift and effective operational cooperation on incidents and sharing of information about risks;

- Ensuring organisations within those vital sectors of our economy are effectively managing the security of their network and information systems. Organisations within those sectors that are identified by Member States as “Operators of Essential Services (OES)” will have to:

    - take appropriate and proportionate technical and organisational measures to manage the security of their network and information systems (including managing cyber security risks and broader security and resilience risks to network and information systems);
    - take appropriate measures to prevent and minimise the impact of incidents affecting the security of their network and information systems;
    - notify the relevant authority of any incidents affecting network and information systems which have a significant impact on the continuity of the essential service they provide.

2.2 The Directive applies to those sectors which are vital for the economy and society, providing services such as the supply of electricity, water and the provision of healthcare and transport.

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

2.4 Designation of organisations as operators of the essential service (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.

2.5 Drinking water supply and distribution has been designated an essential service within Schedule 1 of the NIS Regulations 2018 with the thresholds for an OES within this sector, as identified in Schedule 2, as the supplier of potable water to 200,000 or more people

3. COMPETENT AUTHORITIES (Regulation 3)

3.1 Oversight and enforcement for all regulatory decisions in relation to 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.

3.2 The UK Government has decided that a multiple Competent Authorities approach is the most appropriate for the UK as each Competent Authority has a detailed understanding of the associated challenges for their individual sector.

3.3 In general Competent Authorities are responsible for:

- reviewing the application of the NIS Regulations in their sector or region;
- preparing and publishing guidance to assist OESs 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 Regulations;
- 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

3.4 For the water sector, the designated Competent Authority is the Secretary of State for Environment, Food and Rural Affairs (for England) and Welsh Minsters (for Wales). Their main functions within the Regulations include:

- Setting the policy of the NIS Regulations within the sector
- Providing incident support for non-cyber incidents
- Responsibility of designating additional OES's who do not automatically meet the threshold requirement in Schedule 2
- Power to revoke OES designation

3.6 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 for Environment, Food and Rural Affairs and Welsh Minsters under Section 86(1)(b) of the Water Industry Act 1991 (the 1991 Act), as amended. These functions include:

- Preparing and publishing guidance documents to assist OES's
- To keep and review the list of designated OES in England and Wales
- Defining incident thresholds for incident notification
- Receiving incident notifications and undertaking incident assessments
- Assessing compliance against the Regulations across the sector
- Conducting Inspections (audits)
- Enforcement (including issuing notices and penalties)

3.7 For the other devolved administrations, the Competent Authority function for water is performed by The Drinking Water Quality Regulator (DWQR) in Scotland and The Department of Finance in Northern Ireland.

3.8 Competent Authorities will be supported by the National Cyber Security Centre (NCSC) who will offer technical advice to Competent Authorities, and will conduct the duties of the SPOC and the CSIRT (Section 4).

4. THE NATIONAL CYBER SECURITY CENTRE (NCSC) (Regulations 4 and 5)

4.1 The National Cyber Security Centre (NCSC) has several critical roles to play in support of NIS implementation. It has been designated the national Single Point of Contact (SPOC), the Computer Security Incident Response Team (CSIRT), and the national technical authority.

4.2 As the SPOC (regulation 4), 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 cross-border incidents.

4.3 As the CSIRT (regulation 5), the NCSC will be responsible for cyber incident response, including monitoring incidents, providing dynamic incident analysis and situational awareness as well as providing early warning alerts and announcements. These are not new functions for the NCSC as it already undertakes these roles at a national level for cyber security incidents.

4.4 The NCSC is also the national technical authority and will be supporting OES and Competent Authorities by:

- Publishing a set of cyber security principles for securing essential services,
- Publication of a collection of supporting guidance related to each security principal,
- Producing a Cyber Assessment Framework (CAF) incorporating indicators of good practice,
- Implement guidance and support to Competent Authorities to enable them to:
  - adapt the NCSC NIS principles for use in their sectors
  - plan and undertake assessments using the CAF and interpret the results

4.5 It is important to note that all of these roles are advisory, and the NCSC has no regulatory role within the NIS Regulations. It will not be able to, or seek to, enforce any actions on an OES; this will solely be the responsibility of the Competent Authorities.

5. IDENTIFICATION AND REVOCATIONS OF OPERATORS OF ESSENTIAL SERVICES (Regulations 8 & 9)

5.1 Under regulation 8(1) a water company that meets the threshold outlined in Schedule 2 of the NIS Regulations is designated a OESs within that sector.

5.2 A water company that does not meet the requirements of regulation 8(1) may still be designated an OES if that company meets the conditions outlined in regulation 8(3) and taking into account the information in regulation 8(4). Water company designation in to the scope of NIS under this regulation is the responsibility of the Secretary of State for Environment, Food and Rural Affairs (for England) or via consultation with DWI and Welsh Minsters (for Wales).

5.3 Under regulation 8(8) the DWI and the Secretary of State for Environment, Food and Rural Affairs (for England) and DWI (for Wales) will hold a list of all companies who have been designated an OES. This list is subject to review at regular intervals with the first review taking place before 9 May 2020, with subsequent reviews taking place, at least, every two years. The basis of the review will be for companies to re-confirm that they meet the threshold IN Schedule 2.

5.4 Even if a water company satisfies the threshold mentioned in regulation 8(1)(b), the Secretary of State for Environment, Food and Rural Affairs (for England) or Welsh Minsters (for Wales) via consultation with DWI may, under regulation 9, revoke the designation of that company, by notice, if they conclude that an incident affecting the provision of the essential service by that company is not likely to have significant disruptive effects.

5.5 A water company designated an OES under regulation 8(3) can also have its designation revoked if, by notice, the conditions no longer apply to that company.

5.6 Before a company's designation is revoked The Secretary of State for Environment, Food and Rural Affairs (for England) or Welsh Minsters (for Wales) will:

- serve a notice in writing of proposed revocation on that company;
- provide reasons for the proposed decision;
- invite that company to submit any written representations about the proposed decision
- within such time period as may be specified by the competent authority; and consider any representations submitted by the person under sub-paragraph (c) before a final decision is taken to revoke the designation.

6. SECURITY DUTIES OF OPERATORS OF ESSENTIAL SERVICE (Regulation 10)

6.1 OES must take appropriate and proportionate measures to manage risks to their network and information systems and to prevent and/or minimise the impact of incidents to those systems.

6.2 Water companies understand their own network and information systems and the level of security required and therefore should be capable of taking informed, balanced decisions about how these measures are managed.

6.3 The view for the water sector is that a principles-based approach is the most effective way of driving improvements around the resilience of cyber security in the context of the NIS Regulations rather than an approach based on prescriptive rules. This is because prescriptive rules can lead to unintended consequences, misallocation of resource and limited benefit.

6.4 To aid compliance with regulation 10, the NCSC has defined 14 outcome based security principles that, collectively, describes good cyber security for operators of essential services. These principles have been grouped into 4 top-level objectives:

- Objective A. Managing security risk
- Objective B: Protecting against cyber attack
- Objective C: Detecting cyber security events
- Objective D: Minimising the impact of cyber security incidents

6.5 The 14 principles should be relevant to all network and information systems that support the delivery of the essential service including Industrial Control Systems and any legacy equipment which continues to play a central role.

6.6 Alongside these principles NCSC has also published a collection of guidance documents and reference links which provides further information on how an OES may achieve the outcomes specified in the principals. A summary of the Objectives, Principles and relevant Guidance is outlined in Annex 1 and also available within the NIS Guidance suite on the NCSC Website.

6.7 The NCSC's principles and guidance are primarily focused on ensuring adequate cyber security risk management. However, OES also need to take into account broader resilience risks when considering the security of their network and information systems and these should be included in any risk management plan which demonstrates those risks have been assessed and understood, and mitigation measures put in place where appropriate.

6.8 Some elements of resilience are covered or referenced already within the NCSC principles and guidance such as physical access control (within B.2) or building resilience against system failure (within B.5). Companies should supplement this with robust Business Continuity Plans which will allow the company to respond to a resilience issue that affects network systems.

6.9 It should be noted that NIS requirements do not apply directly to the supply chains of OES. It is the responsibility of the OES to put in place appropriate and proportionate measures, and to ensure that suppliers have in place appropriate measures, to manage risks of their services being disrupted via their supply chain.

Annex 1: Objectives, Principles and Guidance

Objective A. Managing Security Risk

Principle	Principle Overview	Guidance and further References
A1. Governance	Putting in place the policies and processes which govern your organisations approach to the security of network and information systems.	NCSC Introduction to Security Governance ISO/IEC 27001:2013 IEC 62443-2-1:2010
A2. Risk Management	Identification, assessment and understanding of security risks. And the establishment of an overall organisational approach to risk management.	NCSC Risk Management Guidance NCSC assurance blog NCSC Penetration Testing Guidance NCSC Cloud Security Collection: Having confidence in cyber security NCSC Risk frameworks and methods
A3. Asset management	Determining and understanding all systems and/or services required to maintain or support essential services.	ISO/IEC 27001:2013 ISO 55001:2014 - Asset Management ITIL
A4. Supply chain	Understanding and managing the security risks to networks and information systems which arise from dependencies on external suppliers.	NCSC Supply Chain Security NCSC cloud security principle 8: supply chain Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR)

Objective B. Defending systems against cyber attack

Principle	Principle Overview	Guidance and further References
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.	CPNI's Personnel and People Security ISO/IEC 27002:2013 section 5 & 7 IEC 62443-2-1:2010 section 5.8 & IEC 62443-2-1:2010 section 4.3.2.6 SANS blog post SANS security policy templates HP & University College London whitepaper The Compliance Budget
B2. Identity and access control	Understanding, documenting and controlling access to essential services systems and functions.	CPNI physical security guidance NCSC Security Design Principles for Digital Services NCSC Introduction to identity and access management ISO/IEC 27002:2013 section 9 IEC 62443-2-1:2010 NIST Identity and Access Management publications
B3. Data Security	Protecting stored or electronically transmitted data from actions that may cause disruption to essential services.	NCSC 10 Steps Mobile devices and removable media NCSC End user device management guidance ISO/IEC 27002:2013 section 8 IEC 62443-2-1:2010 section 4.3.4.4 ENISA Big Data Security (2016)

B4. System security	Protecting critical network and information systems and technology from cyber-attack.	NCSC Reducing the impact of common cyber attacks IEC 62443-2-1:2010 ISO/IEC 27002:2013 NCSC 10 Steps malware prevention NCSC penetration testing guidance NCSC obsolete platform guidance NCSC Secure by default platforms
B5. Resilient Networks & Systems	Building resilience against cyber-attack.	ISO/IEC 27002:2013 section 17 PD ISO 27019:2013 section 14 IEC 62443-2-1:2010 IEC 62443-2-1:2010 section 4.3.2 HMG Emergency preparedness HMG Emergency Response and Recovery BCI introductory business continuity guidance
B6. Staff Awareness & Training	Appropriately supporting staff to ensure they can support essential services' network and information system security.	CPNI's guidance on developing a security culture GCHQ certified training scheme NCSC 10 Steps: User Education and Awareness

Objective C. Detecting cyber security events

Principle	Principle Overview	Guidance and further References
C1. Security Monitoring	Putting in place the policies and processes which govern your organisations approach to the security of network and information systems.	NCSC 10 Steps: Monitoring NCSC - SOC Buyer's Guide CREST - Protective Monitoring Guidance NIST - Continuous Security Monitoring NIST Guide to Intrusion Detection and Intrusion Prevention Systems ISO/IEC 27002:2013 / 27019 IEC 62443-2-1:2010

C2. Proactive Security Event Discovery	Identification, assessment and understanding of security risks. And the establishment of an overall organisational approach to risk management.	NCSC Pro-active Security Event Discovery

Objective D. Minimising the impact of cyber security incidents

Principle	Principle Overview	Guidance and further References
D1. Response and Recovery Planning	Putting in place the policies and processes which govern your organisations approach to the security of network and information systems.	NCSC 10 Steps: Incident Management NIST Computer Security Incident Handling Guide Part 4 of CREST Cyber Security Incident Response Guide Part 4 ISO 27035 CIR scheme
D2. Improvements	Identification, assessment and understanding of security risks. And the establishment of an overall organisational approach to risk management.	Chapter 8 of ENISA Good Practice Incident Management Guide Parts 2-3 of ISO 27035 Section 3 of NIST Computer Security Incident Handling Guide Part 6 of CREST Cyber Security Incident Response Guide