


| | |
|---|---|
|  | GUIDANCE ON THE IMPLEMENTATION OF THE NETWORK AND INFORMATION SYSTEMS (NIS) REGULATIONS 2018 IN ENGLAND AND WALES |
| Issue Number | 1.0 |
| Date Approved/Released | 25/09/2025 |
| Review Date | 25/09/2026 |
| Procedure Owner | NIS Principal Inspector, DWI |
| Purpose | The purpose of this document is to support drinking water companies who are designated as Operators of an Essential Service (OES companies) under the Network and Information Systems (NIS) Regulations (2018) interpret the NIS regulations and their duties contained within. |

Contents

Document Control3

Introduction and Purpose4

The Network and Information Systems (NIS) Regulations 20184

Overview of the NIS Regulations 2018 Requirements5

Part 1: Introduction6

Part 2: The National Framework8

Part 3: Operators of Essential Services12

Part 4: Digital Services19

Part 5: Enforcement and Penalties19

Part 6: Miscellaneous34

Annex A: Designated Competent Authorities39

Annex B: Essential Services and Threshold Requirements400

Document Control

| Issue Number | Issue Date | Issued By | Change Description |
|--------------|------------|-----------|----------------------------|
| 1.0 | 25/09/2025 | DWI | Final Draft and Published. |

Introduction and Purpose

- 1.1 This Guidance Document has been issued by the Drinking Water Inspectorate (the Inspectorate) to support water companies, designated as an Operator of Essential Service (OES), in complying with the Network and Information Systems Regulations 2018 (the NIS Regulations). It sets out the core obligations placed upon an OES under the NIS Regulations and clarifies the responsibilities each water company must fulfil in order to protect the essential service of supplying drinking water.
- 1.2 The aim of this Guidance is to explain how an OES should interpret and implement the NIS Regulations within the water sector, ensuring that the availability, integrity and confidentiality of network and information systems are appropriately managed. Compliance not only helps each water company meet its statutory duties but also contributes to maintaining public confidence in the provision of safe and clean drinking water.
- 1.3 This Guidance is published on behalf of the Secretary of State for Environment, Food and Rural Affairs (Defra) and Welsh Ministers in accordance with regulation 3 of the NIS Regulations. The Inspectorate has been appointed as the Competent Authority (CA) for the sector, responsible for overseeing and enforcing the requirements of the NIS Regulations in England and Wales.
- 1.4 This document forms part of a suite of resources available from the Inspectorate. Further Guidance Documents are accessible via Resilience Direct and on the Inspectorate's website (in the case of the [NIS Enforcement Policy](#)) and include:
 - Incident Reporting Requirements
 - Latest CAF Return Blank Templates
 - Network and Information Systems Regulations Enforcement Policy
 - Roles and Responsibilities under the NIS Regulations
 - The Cyber Assessment Framework (CAF) (Annually Updated) (CAF Guidance 2025)
- 1.5 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.

The Network and Information Systems (NIS) Regulations 2018

- 2.1 The NIS Regulations aims to improve the security of network and information systems that support or have a direct effect on the production and delivery of wholesome water (the essential service). They were laid before Parliament on 20 April 2018 and came into force on 10 May 2018. An amendment to the NIS Regulations 2018 was laid before Parliament on 10 November 2020 and came into force on 31 December 2020. By imposing legal duties on Operators of Essential Services (OES) and relevant Digital Service Providers, the Regulations seek to ensure that the risk of disruption to vital services - such as water, transport, energy, health and digital infrastructure is effectively managed.
- 2.2 The NIS Regulations recognise that failures or compromises of network and information systems can have **significant** consequences for businesses, citizens and public services. To address this, they mandate that OES' implement **appropriate** and **proportionate** measures to prevent, detect and respond to incidents that threaten the availability, integrity or confidentiality of these

systems. The definition of a network and information system is outlined under Regulation 1 (2) and is considered to include electronic communications networks; any device or group of interconnected or related devices which perform automatic processing of digital data; or digital data stored processed, retrieved or transmitted by an electronic network or device.

2.3 For the water sector this definition can apply to both Operational Technology (OT) systems and Information Technology (IT) systems.

2.4 The Inspectorate, as Competent Authority, has mandated the use of the Cyber Assessment Framework (CAF) developed by the NCSC, as a framework for OESs. OESs are expected to submit a self-assessment annually to the Inspectorate, demonstrating their maturity against the designated Sector Specific Profile (SSP) and Enhanced CAF Profile (eCAF). In other sectors, these profiles are commonly referred to as 'Basic Profile' and 'Enhanced Profile', respectively. Whilst the CAF is not a requirement of the NIS regulations, the framework sets out key principles with outcomes that are referred to as indicator statements or Indicators of Good Practice (IGPs), enabling OESs to demonstrate that they have the necessary organisational, technical and procedural controls in place

2.5 For further guidance on the CAF, please refer to the latest version of to THE CYBER ASSESSMENT FRAMEWORK (CAF) 2025 (CAF Guidance 2025).

Overview of the NIS Regulations 2018 Requirements

3.1 The below sections provide an overview of the key obligations set out in the Regulations, outlining the responsibilities of OES' and how compliance is to be demonstrated. The requirements apply to both Operational Technology (OT) and Information Technology (IT) systems that are integral to the production and supply of wholesome drinking water.

3.2 Each Section, Article, Annex and Regulation has been summarised to provide clarity on its intent, scope and practical implications for OES. Where necessary, references to further guidance have been provided to support implementation.

3.3 The guidance listed below is **only** applicable to the drinking water sector in England and Wales, as per the scope of the Inspectorate's activities. Other Sections, Articles, Annexes and Regulations not relevant to the drinking water sector, or to England and Wales have been purposely omitted from the guidance. To view the latest revision of the Regulation in full, please click [here](#).

Part 1: Introduction

| Regulation | Guidance |
|---|--|
| Citation, commencement, interpretation and application | |
| 1.—(1) These Regulations may be cited as the Network and Information Systems Regulations 2018 and come into force on 10th May 2018. | The Network and Information Systems Regulations 2018 establish legal requirements for the security and resilience of network and information systems that support essential services, including the supply of drinking water. They were introduced to strengthen protection against cyber threats and system failures that could disrupt critical infrastructure. The Regulations came into force on 10 May 2018, meaning all designated Operators of Essential Services (OES) have been subject to compliance obligations since that date. |
| 1.—(2) In these Regulations— (Definitions of key terms such as ‘cloud computing service’, ‘digital service provider’, ‘essential service’, ‘incident’, and ‘network and information system’.) | <p>This section provides definitions of key terms used throughout the Regulations. These definitions clarify the scope of the legislation and ensure consistent interpretation. Definitions include:</p> <ul style="list-style-type: none"> • Essential service: A service critical to societal or economic activities, including the supply of wholesome drinking water. • Incident: Any event that has an adverse effect on the security of network and information systems. • Network and Information System (NIS): This includes IT and Operational Technology (OT) systems that store, process, or transmit digital data essential to the operation of an essential service. <p>Understanding these definitions is fundamental to ensuring compliance, as they determine the applicability of the Regulations to different systems and operations within the water sector.</p> |
| 1.—(3) References to Articles, Regulations, and Authorities | This provision clarifies references to other legislation and regulatory bodies. The Inspectorate, on behalf of the Secretary of State for Environment, Food and Rural Affairs (Defra), is designated as the Competent Authority (CA) responsible for overseeing compliance with the Regulations in the water sector in England and Wales. Other references, such as the Computer Security Incident Response Team (CSIRT) network, indicate coordination between UK authorities and European cyber security bodies. |

| | |
|---|--|
| 1.—(4) Interpretation of Terms in Directive 2016/1148 | Where terms in the Regulations are also used in Directive 2016/1148 (EU NIS Directive), they retain the same meaning, therefore ensuring continuity with the UK NIS Regulations EU counterpart. |
| 1.—(5) National Security and Law Enforcement Considerations | This section establishes that compliance with the Regulations does not override obligations related to national security, law enforcement, or public safety. OES' must balance regulatory compliance with responsibilities to protect sensitive information and cooperate with law enforcement agencies where necessary. |
| 1.—(6) Geographic Scope of the Regulations | The Regulations apply to the entire United Kingdom, including its internal waters, territorial sea, and designated areas of the continental shelf. This ensures that network and information systems supporting essential services within these areas are subject to regulatory oversight. |

Part 2: The National Framework

| Regulation | Guidance |
|---|--|
| The NIS National Strategy | |
| 2.—(1) A Minister of the Crown must designate and publish a strategy to provide strategic objectives and priorities on the security of network and information systems in the United Kingdom ("the NIS national strategy"). | The NIS national strategy establishes the UK's overarching approach to the security and resilience of network and information systems. It is developed by the UK Government and sets out the strategic objectives and priorities that guide regulatory oversight, industry compliance, and national preparedness. This strategy provides the framework within which OES', including water companies, must operate to ensure the protection of critical infrastructure . |
| 2.—(2) The strategic objectives and priorities set out in the NIS national strategy must be aimed at achieving and maintaining a high level of security of network and information systems in— (a) the sectors specified in Schedule 1 ("the relevant sectors"); and (b) digital services. | The strategy applies to essential services , including the water sector, and outlines national priorities for achieving a high level of baseline security. It also extends to digital services such as cloud computing providers, ensuring that critical digital infrastructure is protected. The water sector's obligations under the strategy align with national efforts to improve cyber security and resilience against system failures and cyber threats. |
| 2.—(3) The NIS national strategy may be published in such form and manner as the Minister considers appropriate. | The UK Government determines how and where the NIS national strategy is published. This ensures flexibility in updating the strategy and making it accessible to relevant stakeholders, including regulators and OES'. |
| 2.—(4) The NIS national strategy may be reviewed by the Minister at any time and, if revised, must be published as soon as reasonably practicable. | The national strategy is subject to periodic review to reflect emerging threats, technological advancements, and changes in regulatory priorities. Any updates must be published in a timely manner, ensuring that OES' and regulators work from the most current guidance. The most up to date guidance is available from NCSC here . |
| 2.—(5) The NIS national strategy must address the following matters— (a) regulatory measures and enforcement framework; (b) roles and responsibilities of key persons; (c) preparedness, response and recovery measures; (d) education, awareness, and training programmes; (e) research and development plans; (f) risk assessment plans; (g) a list of persons involved in implementation. | <p>The national strategy provides a detailed framework for managing network and information security risks.</p> <p>The national strategy outlines how compliance is monitored and enforced, ensuring OES meet their obligations.</p> <ul style="list-style-type: none"> • It clarifies who is responsible for implementing security measures. • It covers how OES' should prepare for, detect, and recover from security incidents. • It supports ongoing awareness and capability development within the CNI sector. |

| | |
|--|---|
| 2.—(7) Before publishing the NIS national strategy, the Minister may redact any part of it which relates to national security. | Certain elements of the strategy may be withheld from public publication if they contain sensitive information related to national security. Typically, this would be classified at 'SECRET' or above, in line with the Government Security Classification Policy (GSCP) , and is therefore subject to specific handling requirements. This ensures that critical security measures are not exposed to potential adversaries. |
|--|---|

| Regulation | Guidance |
|---|---|
| Designation of national competent authorities | |
| 3.—(1) The person specified in column 3 of Schedule 1 is designated as the competent authority for the subsector specified in column 2 of that table ("the designated competent authorities"). | The Drinking Water Inspectorate is the Competent Authority for the water sector in England and Wales, as designated by the Secretary of State for Environment, Food and Rural Affairs. The Inspectorate is responsible for enforcing compliance with the NIS Regulations, ensuring that water companies implement necessary security measures. Other competent authorities oversee different sectors and have been excluded from this guidance document. A full list of competent authorities can be found on the GOV.UK website (Annex I: List of Competent Authorities), or below in Annex A . |
| 3.—(3) The Competent Authority must— (a) review the application of these Regulations; (b) prepare and publish guidance; (c) maintain a list of designated OES'; (d) maintain a list of revoked designations; (e) provide these lists to GCHQ; (f) consult with the Information Commissioner for personal data breaches; (g) co-operate with other authorities, including law enforcement, GCHQ, and CSIRT. | The Inspectorate, in their role as competent authority, is required to review and monitor the implementation of the NIS Regulations in the water sector. This includes: <ul style="list-style-type: none"> • Maintaining an up-to-date list of designated OES and any revocations. • Publishing guidance to help OES understand their obligations. • Collaborating with government and cyber security bodies, including GCHQ (acting as the Single Point of Contact - SPOC), NCSC, Cabinet Office and the CSIRT. • Working with law enforcement and the Information Commissioners Office where security incidents involve personal data breaches. |

| Regulation | Guidance |
|--|---|
| Designation of the single point of contact | |
| 4.—(1) GCHQ is designated as the SPOC on the security of network and information systems for the United Kingdom. | GCHQ serves as the SPOC for NIS-related security matters. It facilitates coordination between regulatory bodies, enforcement agencies, and other relevant stakeholders. |
| 4.—(2A) The SPOC must— (a) consult and co-operate with law enforcement; (b) work with enforcement authorities to support regulatory enforcement. | GCHQ is responsible for coordinating national-level responses to cyber threats. It liaises with law enforcement and regulatory bodies to enhance the UK's cyber security posture. |

| Regulation | Guidance |
|--|--|
| Designation of computer security incident response team | |
| 5.—(1) GCHQ is designated as the CSIRT for the United Kingdom. | GCHQ also operates as the CSIRT, tasked with monitoring, detecting, and responding to cyber security threats. |
| 5.—(2) The CSIRT must— (a) monitor incidents; (b) provide alerts and guidance; (c) respond to incident reports; (d) conduct risk analysis; (e) collaborate with private sector partners; (f) promote standardised incident management practices. | <p>The CSIRT provides threat intelligence and response coordination. It is responsible for:</p> <ul style="list-style-type: none"> • Detecting and analysing security incidents affecting essential services. • Issuing alerts and advisories to stakeholders. • Coordinating responses to significant cyber security incidents. <p>Supporting OES' in mitigating risks and improving their overall cyber security posture.</p> |

| Regulation | Guidance |
|---|--|
| Information sharing – enforcement authorities | |
| 6.—(1) NIS enforcement authorities may share information with law enforcement, the CSIRT, and relevant EU authorities if necessary for enforcement or national security purposes. | <p>Information sharing is permitted (where necessary) to support cyber security enforcement and incident response activities. However, data protection principles apply, ensuring that shared information is limited to what is relevant and proportionate. Any data related to cyber resilience across the water sector is likely to be shared at a high level, on a need-to-know basis, and anonymised.</p> <p>The Inspectorate has a memorandum of understanding (MOU) with the NCSC in relation to data sharing, ensuring that a framework is in place for the provision of sharing data with the appointed Technical Authority.</p> |

| | |
|--|--|
| <p>6.—(2) When sharing information with an EU authority, NIS enforcement authorities are not required to share—</p> <p>(a) confidential information;</p> <p>(b) information that may prejudice security or commercial interests.</p> | <p>Due to the UK’s withdrawal from the European Union (EU), this provision protects sensitive commercial and security information from being shared unnecessarily with foreign entities. Information is only shared where it directly supports regulatory enforcement or national security objectives.</p> |
|--|--|

Part 3: Operators of Essential Services

| Regulation | Guidance |
|---|--|
| Identification of operators of essential services | |
| 8.—(1) If a person provides an essential service listed in Schedule 2 (Appendix B), relies on network and information systems, and meets the threshold requirements, they are deemed to be designated as an Operator of Essential Services (OES). | <p>Water companies that supply drinking water are classified as Operators of Essential Services under the NIS Regulations. To be designated as an OES, an organisation must:</p> <ul style="list-style-type: none"> • Provide an essential service (such as drinking water supply and distribution). • Rely on network and information systems (such as IT and OT systems used for monitoring and control). • Meet the threshold requirements as outlined in the Regulations. * <p>Once designated as an OES, a water company must comply with the security and incident reporting obligations under the Regulations and any associated guidance provided by the competent authority.</p> <p>*The threshold requirement which applies to the essential service of the supply of potable water in the United Kingdom is the supply of water to 200,000 or more people. For further information, please see Schedule 2 (Annex B).</p> |
| 8.—(2) A person who falls within paragraph (1) must notify the designated competent authority in writing before the notification date. | A water company and/or potential OES' must formally notify the Inspectorate (as the Competent Authority for the water sector in England and Wales) of their designation. This ensures that the Inspectorate maintains an up-to-date record of all regulated entities and can oversee compliance effectively. Currently, there are 17 designated companies within the scope of the NIS regulations across England and Wales. If there are any major changes to population served, companies must inform the Inspectorate. |
| 8.—(3) The Competent Authority may designate a person as an OES even if they do not meet the threshold requirements, if an incident affecting their service could have significant disruptive effects. | Defra and Welsh Government have the authority to designate additional entities as OES' if their services are deemed critical to the delivery of drinking water and their failure would have a significant impact. This allows for flexibility in regulating essential service providers that may not initially meet automatic threshold criteria but still pose a high risk to the security of the drinking water supply. |
| 8.—(4) When determining whether an entity should be designated as an OES under paragraph | The Inspectorate will assess and determine whether a water company or associated service provider should be designated as an OES based on |

| | |
|---|--|
| <p>(3), the Competent Authority must consider factors such as:</p> <p>(a) The number of users reliant on the service.</p> <p>(b) The dependency of other sectors on the service.</p> <p>(c) The potential impact of incidents in terms of severity and duration.</p> <p>(d) The entity's market share.</p> <p>(e) The geographical area affected.</p> <p>(f) The availability of alternative providers.</p> <p>(g) The consequences for national security.</p> <p>(h) Any other relevant factors.</p> | <p>the potential risk and impact of a network or information system failure. Key considerations include:</p> <ul style="list-style-type: none"> • Number of customers affected - Larger providers serving a significant population are more likely to be designated. • Impact on other critical sectors - If failure could disrupt healthcare, food production, or emergency response, designation is more likely. • Market share and availability of alternatives - A provider with no viable alternative will be prioritised for designation. • Geographical coverage - Rural areas with limited backup supply options may require higher security measures. • National security implications - Any service that could impact public safety or infrastructure stability is considered critical. |
| <p>8.—(5) The Competent Authority must formally notify an entity of their OES designation in writing and provide reasons for the decision.</p> | <p>If a water company is formally designated as an OES, it will receive an official written notice from the Inspectorate, explaining why it has been identified as critical to the drinking water supply sector, and their responsibilities under the NIS Regulations.</p> |
| <p>8.—(7A) If an OES believes it no longer meets the designation criteria, it must notify the Competent Authority with supporting evidence.</p> <p>8.—(7B) The Competent Authority must review this evidence and decide whether to revoke the designation.</p> | <p>OES' that no longer meet the requirements for designation (e.g. due to structural changes, reduced reliance on network systems, insolvency and/or administration, mergers and acquisitions or outsourcing of critical functions) must inform the Inspectorate. The Inspectorate will then assess whether revocation is appropriate. However, an OES cannot unilaterally revoke its designation - it remains regulated until the Inspectorate on behalf of Defra or Welsh Government issues an official letter of revocation.</p> |
| <p>8.—(8) The Competent Authority must maintain a list of all designated OES and review it at regular intervals, at least every two years.</p> | <p>The Inspectorate must maintain and update a list of all regulated OES' and conduct reviews every two years to ensure that the designation remains valid and relevant to evolving risks.</p> |

| Regulation | Guidance |
|---|---|
| Nomination by an OES of a person to act on its behalf in the United Kingdom | |
| 8A.—(1) If an OES is headquartered outside the UK but provides essential services within the UK, it must nominate a representative within the UK to act on its behalf. | <p>All water companies in England and Wales will be a UK registered entity under the current industry model. This requirement should therefore not apply to any OES within the Inspectorate's scope.</p> <p>OES' with parent group owners located outside of the UK must have regard to the relevant UK National Security policies in undertaking its NIS responsibilities.</p> |
| 8A.—(2) An OES falls within this paragraph if they have received a notice in writing from a designated competent authority for the OES requiring them to comply with this regulation. | If an OES were to be included in scope of this requirement, they will receive an official written notice from the Inspectorate, explaining their requirement to comply with this regulation under the NIS Regulations. |
| 8A.—(3) The nominated representative must provide their contact details (including their name, the name and address of the nominated person, and up-to-date contact details of the nominated person (including email addresses and telephone numbers)) to the Competent Authority and update them within seven days of any changes. | <p>The nominated person's details must be kept up to date, ensuring that the Inspectorate and GCHQ can reach them when necessary for regulatory, enforcement, or cyber security matters.</p> <p>A Nominated Person under 8A (3) relates to the designated Board Level Contact and Day to Day Contact for an OES for the Water Sector.</p> <p>The Annual CAF return's board declaration requires the latest statement of board-level and day to day designated persons with contact details. Mid-year personnel changes must be communicated to the Inspectorate at the earliest convenience.</p> |

| Regulation | Guidance |
|--|---|
| Revocation | |
| 9.—(1) The Competent Authority may revoke an OES designation if it determines that an incident affecting the service would no longer have a significant disruptive effect. | If a water company no longer presents a significant risk to essential service delivery (e.g. due to improved redundancy measures or reduced operational scope), the Inspectorate, on behalf of Defra or the Welsh Government, may remove it from the list of designated OES'. |
| <p>9.—(3) Before revoking an OES designation, the Competent Authority must—</p> <p>(a) Serve a notice of proposed revocation.</p> <p>(b) Provide reasons for the decision.</p> <p>(c) Allow the OES to submit written representations.</p> | <p>The revocation process is formal and allows OES' to challenge the decision. If an OES believes it should remain designated, it can submit supporting evidence before a final determination is made.</p> <p>The Inspectorate will formally write to an OES confirming final revocation.</p> |

| | |
|---|---|
| (d) Consider any representations before making a final decision. | |
| 9.—(4) The Competent Authority must consider the same factors listed in Regulation 8(4) when deciding whether to revoke an OES designation. | The same risk-based approach used to designate an OES must be applied when considering revocation, ensuring consistency in the Inspectorate's regulatory decisions. |

| Regulation | Guidance |
|---|---|
| The security duties of operators of essential services | |
| 10.—(1) An OES must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies. | <p>OES' must implement risk-based security controls to protect the network and information systems essential for the delivery of drinking water. Examples including, but not limited to:</p> <ul style="list-style-type: none"> • Cyber security policies and procedures to manage threats. • Risk assessments, including regular cyber and operational risk assessments. • Logical and physical access controls to restrict unauthorised access to key networks and sites. • System monitoring tools to detect anomalies and potential security breaches. • Incident response and business continuity plans to ensure effective mitigation of disruptions. • Network segmentation to isolate critical operational systems (OT) from enterprise IT networks. • Regular security patching and vulnerability management to address known threats. • Security awareness training programmes for employees, contractors, and third-party suppliers. • Secure backup and recovery solutions, ensuring data integrity and rapid restoration in the event of cyber incidents. • Supply chain security controls, including vetting and assurance for third-party service providers managing sensitive infrastructure. |
| 10.—(2) An OES must take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services. | <p>OES' must ensure service continuity by:</p> <ul style="list-style-type: none"> • Implementing security defences to prevent cyber threats. • Regularly patching and updating systems to mitigate vulnerabilities. |

| | |
|--|---|
| | <ul style="list-style-type: none"> • Developing and testing incident response plans to minimise downtime. • Deploying and testing backup and recovery solutions to restore services quickly. • Review the root cause and contributing factors of operational incidents to prevent or reduce the risk of a reoccurrence or similar incident occurring in the wider operational estate. |
| 10.—(3) The measures taken under paragraph (1) must, having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risk posed. | <p>OES' must follow best practices and ensure their security measures align with the latest technological advancements, taking a holistic approach that integrates cyber, physical and personnel security. This means:</p> <ul style="list-style-type: none"> • Implementing modern cyber/information security frameworks, including, but not limited to: <ul style="list-style-type: none"> ○ Cyber Assessment Framework ○ Cyber Essentials/Cyber Essentials + ○ ISA/IEC 62443 ○ NIST SP 800-53 ○ CIS Controls (CIS 18) • Adopting industry standards (e.g. ISO 27001, NCSC or NPSA guidance etc.). • Ensuring continuous security improvements based on new threats. |
| 10.—(4) Operators of essential services must have regard to any relevant guidance issued by the relevant competent authority when carrying out their duties imposed by paragraphs (1) and (2). | <p>OES' must comply with guidance issued by the Inspectorate (such as this document, and supporting documentation referenced in 1.4) and other relevant authorities to ensure that security measures meet sector-specific and regulatory requirements and/or targets.</p> <p>Guidance may be given in different formats not restricted to- letters to all of the industry, letters to specific OESs, verbally, by email, in published guidance, or through enforcement activity as relevant (eg. DWI Recommendations, Requirements and suggestions or formal Notices).</p> |

| Regulation | Guidance |
|---|--|
| The duty to notify incidents | |
| 11.—(1) An OES must notify the designated competent authority in writing about any incident which has a significant impact on the continuity of the essential service it provides (“a network and information systems (“NIS”) incident”). | <p>If a security incident disrupts water services, the OES must report it to the Inspectorate. This ensures:</p> <ul style="list-style-type: none"> • Regulatory oversight of security events. • Timely response to mitigate impact. • Coordination with other government authorities (such as NCSC or the ICO) to manage large-scale incidents. |

| | |
|--|---|
| | The Inspectorate's reporting guidance for NIS-related incidents is contained within the Incident Reporting Requirements guidance document (see 1.4) and covers a broader definition of thresholds of incident to report. |
| <p>11.—(2) In order to determine the significance of the impact of an incident, an OES must have regard to the following factors—</p> <p>(a) The number of users affected by the disruption of the essential service.</p> <p>(b) The duration of the incident.</p> <p>(c) The geographical area affected by the incident.</p> | <p>OES' should assess the severity of an incident based on:</p> <p>The scale of disruption (how many customers are impacted).</p> <p>The duration (short-term outage vs. prolonged service failure).</p> <p>The geographical scope (local vs regional impact). Larger-scale or long-duration incidents are more likely to require notification.</p> |
| <p>11.—(3) (a) The notification must include:</p> <p>(i) the operator's name and the essential services it provides.</p> <p>(ii) the time the NIS incident occurred.</p> <p>(iii) the duration of the NIS incident.</p> <p>(iv) information concerning the nature and impact of the NIS incident.</p> <p>(v) information concerning any, or any likely, cross-border impact of the NIS incident.</p> <p>(vi) any other information that may be helpful to the competent authority.</p> | <p>The incident report must be detailed, covering:</p> <p>What happened (nature of the issue).</p> <p>When it happened (time and duration).</p> <p>How it happened (root cause).</p> <p>Who was affected (users and geographic impact).</p> <p>Whether other regions/countries /sectors were impacted.</p> <p>How the OES responded to restore normal operation/business as usual.</p> <p>An OES must have regard to the latest version of the Inspectorate's Incident Reporting Requirements Guidance document (1.4), which further outlines reporting content and a template to report.</p> <p>It is expected that an OES provides the above information that it can reasonably provide at the time of initial notification to the Inspectorate. Further details can and should be provided as an update when the information becomes available, in line with any agreed incident update frequencies.</p> |
| <p>11.—(3)(b) Notification must be provided to the Competent Authority:</p> <p>(i) Without undue delay and no later than 72 hours after becoming aware of the incident.</p> <p>(ii) In such form and manner as determined by the Competent Authority.</p> | <p>An OES must report NIS and NIS-related incidents within 72 hours of detection, in line with the Inspectorate's Incident Reporting Requirements Guidance documentation threshold. Prompt reporting allows the Inspectorate, and other supporting agencies including Lead Government Departments (LGDs) to:</p> <ul style="list-style-type: none"> • Monitor trends in cyber security threats. • Assist in incident containment. • Coordinate responses and agree/align public messaging where national interests are affected. |

| | |
|--|--|
| | <ul style="list-style-type: none"> • Brief Ministers and officials. |
| <p>11.—(5) After receiving a notification, the Competent Authority must:</p> <p>(a) Assess what further action, if any, is required.</p> <p>(b) Share the NIS incident information with the CSIRT as soon as reasonably practicable.</p> | <p>Once an incident is reported, the Inspectorate assesses its severity and determines necessary follow-up actions. If required, details may be shared with the CSIRT for national security coordination.</p> |
| <p>11.—(6) CSIRT may inform the relevant authorities in a Member State if the incident has a significant cross-border impact.</p> | <p>If an incident has an international (cross-border) impact, UK authorities may share relevant information with European and global cyber security bodies to ensure coordinated response efforts.</p> |
| <p>11.—(7) After receiving a notification, the Competent Authority or CSIRT may:</p> <p>(a) Inform the OES about any relevant information relating to the incident.</p> <p>(b) Inform the public if public awareness is necessary.</p> | <p>The Inspectorate or CSIRT may provide updates to the affected OES regarding the investigation or response efforts. Additionally, if an incident poses a public safety risk, they may issue public notifications to raise awareness and provide guidance to those impacted.</p> <p>The Inspectorate are bound to respond to Freedom Of Information (FOI) requests under the Freedom Of Information Act 2000. The Inspectorate must balance any data release with our right to exemptions under the outlined national security clauses in the Act, section 23 and 24, respectively.</p> |
| <p>11.—(8) Before informing the public, the Competent Authority or CSIRT must consult each other and the OES who provided the notification.</p> | <p>Public disclosure of incidents must be carefully managed to avoid misinformation, spreading undue panic or to undermine public confidence in the quality or wholesomeness of drinking water. The Inspectorate, CSIRT, and OES must coordinate before releasing details publicly.</p> |
| <p>11.—(9) The Competent Authority must provide an annual report to the SPOC identifying the number and nature of NIS incidents notified under paragraph (1).</p> | <p>The Inspectorate must submit an annual report summarising reported incidents when requested, ensuring transparency and national security monitoring. The definition in 11 (1) for incidents is what is classed and counts towards cross-sector statistics in data provided to NCSC annually for incidents, although as mentioned above, the Inspectorate stipulates a broader definition of NIS or NIS-related incidents to be reported.</p> |
| <p>11.—(10) The first report must be submitted by 1st July 2018, with subsequent reports submitted annually.</p> | <p>As the NIS regulations came into force in May 2018, the first Inspectorate report was due by 1st July 2018. Subsequently, the Inspectorate submits and has submitted reports to the SPOC annually, when requested, ensuring a consistent reporting cycle, enabling trend analysis and improvements to the UK's national cyber resilience posture.</p> |
| <p>11.—(11) The CSIRT is not required to share information if it contains—</p> <p>(a) Confidential information.</p> | <p>The protection of sensitive data is a priority. Incident details will not be shared if they could:</p> <ul style="list-style-type: none"> • Expose commercial/trade secrets. |

| | |
|--|--|
| (b) Information that may prejudice the security or commercial interests of an OES. | <ul style="list-style-type: none"> • Compromise national security. • Reveal confidential customer data. |
| 11.—(12) Operators of essential services must have regard to any relevant guidance issued by the Competent Authority when carrying out their duties under paragraphs (1) to (4). | OES' must follow Inspectorate guidance on incident notification guidance- specifically Incident Reporting Requirements guidance documentation (1.4) to ensure proper handling and reporting of security incidents. |

Part 4: Digital Services

Part 4 of the NIS Regulations (Digital Services) focusses on Relevant Digital Service Providers (service providers of online marketplaces, online search engines, and cloud computing services). Whilst in the future, cloud computing services will become prevalent in the water sector, as many water companies move to the cloud with their next generation monitoring and telemetry tools, at time of writing, this does not apply.

Part 5: Enforcement and Penalties

| Regulation | Guidance |
|---------------------|----------|
| Information notices | |

| | |
|---|--|
| <p>15.—(1) A designated competent authority may serve an information notice on any person requiring them to provide information necessary to determine whether they meet the threshold for designation as an OES.</p> | <p>The Inspectorate, as the Competent Authority for the water sector, has the authority to request relevant information from water companies to assess whether they should be designated as an OES. This may include technical, operational, or business data that demonstrates reliance on network and information systems. If the information requested is not provided under an informal request/communication, the Inspectorate may serve an Information Notice to obtain it under this Regulation.</p> <p>The Water Industry Act 1991 designates further rights of entry to the Inspectorate applicable to NIS by virtue of the risk to sufficiency of water supplies. Inspectors are warranted under section 86 of the Water Industry Act, granting them the powers to request information from water companies.</p> <p>Section 86 (3) states that:</p> <ul style="list-style-type: none"> • Without prejudice to the powers conferred by subsection (4) below, it shall be the duty of a water undertaker [water supply licensee] or other relevant person (as defined in section 70(1A) above)— <ul style="list-style-type: none"> ○ (a) to give [an inspector] appointed under this section all such assistance; and ○ (b) to provide [an inspector] so appointed with all such information <p>Section 86 (6) references the penalties in place for water companies (or individuals) who fail to comply with the Inspectorates information notices:</p> <ul style="list-style-type: none"> • Any water undertaker [water supply licensee or other relevant person] which fails to comply with the duty imposed on [that person] by virtue of subsection (3) above shall be guilty of an offence and liable [on summary conviction, or on conviction on indictment, to a fine]. |
| <p>15.—(2) A designated competent authority may serve an information notice on an OES requiring them to provide information to assess their security posture, compliance, or the impact of past incidents.</p> | <p>Water companies designated as OES' must comply with information requests from the Inspectorate. These requests could relate to:</p> <ul style="list-style-type: none"> • Security assessments, such as: <ul style="list-style-type: none"> ○ Compliance with the Cyber Assessment Framework (CAF) ○ Risk assessments for IT and OT security threats |

| | |
|---|--|
| | <ul style="list-style-type: none"> ○ Penetration test reports, vulnerability assessments, and remediation actions • Incident investigations, including: <ul style="list-style-type: none"> ○ Suspected cyber breaches or security compromises ○ Root cause analysis and corrective measures ○ Regulatory reporting of security incidents • Ongoing regulatory oversight, covering: <ul style="list-style-type: none"> ○ Reviews of security measures, policies, and governance ○ Regulatory information that has not been provided in prior submissions ○ Progress on legal notices, including compliance actions and remedial measures ○ Testing schedules, such as business continuity and disaster recovery exercises <p>The information will be obtained by means of a Notice if not provided as expected.</p> |
| 15.—(5) An information notice must include: (a) A description of the required information. (b) The reasons for requesting it. (c) The required format. (d) A deadline for submission. | OES' must respond within the specified timeframe, ensuring that the information is accurate, complete, and formatted correctly as per the Inspectorate's request. Timeframes will vary per information notice, dependant on the level of information requested, and the urgency of the request. |
| 15.—(7) The competent authority may withdraw an information notice by written notice. | The Inspectorate can cancel an information notice if it is no longer necessary or appropriate, ensuring proportionality in their enforcement. |

| Regulation | Guidance |
|--|---|
| Power of inspection | |
| 16.—(1) A competent authority may: (a) Conduct an inspection. (b) Appoint a third party to conduct an inspection. (c) Direct an OES to appoint an approved person to conduct an inspection. | <p>The Inspectorate can conduct audits and inspections (interchangeably used) to assess an OES' compliance with their NIS Security Duties. Inspections can take place in various forms, namely:</p> <ul style="list-style-type: none"> • Internal (Inspectorate-led audits). • External (third-party audits). • Joint (audits conducted by a third-party in collaboration with the Inspectorate) • Self-conducted (OES appointing an approved auditor). |

| | |
|---|--|
| <p>16.—(3) The OES must:</p> <p>(a) Pay the reasonable costs of the inspection [if so required by the relevant competent authority or the Information Commissioner];</p> <p>(b) Co-operate with inspectors.</p> <p>(c) Provide access to premises and documents.</p> <p>(d) Allow examination, printing, copying, or removal of documents.</p> <p>(e) Allow the inspector access to any person from whom the inspector seeks relevant information for the purposes of the inspection.</p> <p>(f) Not intentionally obstruct an inspector performing their functions under these Regulations.</p> <p>(g) Comply with any request made by, or requirement of, an inspector performing their functions under these Regulations.</p> | <p>OES' must fully cooperate during inspections, allowing the Inspectorate access to facilities, systems, and documentation to verify their compliance against the NIS regulations. The Inspectorate recovers costs from any Inspection or Audit activity from OES' under an agreed regulatory cost recovery mechanism, charged annually which has been in use since 2018.</p> <p>“Inspector” means any person conducting all or any part of an inspection in accordance with paragraph (1) or (2). This includes both ‘warranted’ or warrant-card-holding Inspectorate personnel and/or third-parties acting on behalf of the Inspectorate, under regulation 16(1).</p> |
| <p>16.—(5) Inspectors may:</p> <p>(a) At any reasonable time enter the premises of an OES or RDSP (except any premises used wholly or mainly as a private dwelling) if the inspector has reasonable grounds to believe that entry to those premises may be necessary or helpful for the purpose of the inspection.</p> <p>(b) Require an OES or RDSP to leave undisturbed and not to dispose of, render inaccessible or alter in any way any material, document, information, in whatever form and wherever it is held (including where it is held remotely), or equipment which is, or which the inspector considers to be, relevant for such period as is, or as the inspector considers to be, necessary for the purposes of the inspection.</p> <p>(c) Require an OES or RDSP to produce and provide the inspector with access, for the purposes of the inspection, to any such material, document, information or equipment which is, or which the inspector considers to be, relevant to the inspection, either immediately or within such period as the inspector may specify.</p> <p>(d) examine, print, copy or remove any document or information, and examine or remove any material or equipment (including for the purposes of printing or copying any document or information) which is, or which the inspector considers to be, relevant for such period as is, or as the inspector considers to be, necessary for the purposes of the inspection.</p> | <p>Inspectors have broad investigative powers, both from the NIS regulations and the Water Industry Act, which allows them to review the cyber security and operational resilience posture of OES', ensuring compliance with NIS security requirements.</p> <p>Appropriate notice will be given in line with the purpose of the visit, whereby limited notice can be appropriate. The Inspectorate issues an ‘Annual Notice of Intention to Audit’ to OES' under Schedule 6 (6) (2) of the Water Industry Act 1991 by virtue of the powers specified under 86(4) of the Act, plus regulation 16 (1) (a) of the NIS Regulations. This Letter was sent first to Board Contacts on 04 September 2023.</p> <p>OES' are expected to provide any and all relevant materials or information that the Inspectorate requests prior, during and following the inspection.</p> <p>Whilst the Inspectorate can take documentation and equipment offsite, typically, it is requested that all evidence is demonstrated during an inspection. Any further evidence required should be uploaded by the OES to Resilience Direct or whatever manner is requested by the Inspectorate.</p> <p>The Inspectorate can undertake tests (or direct the OES to conduct testing) including but not limited to:</p> |

| | |
|---|--|
| <p>(e) Take a statement or statements from any person.</p> <p>(f) Conduct, or direct the OES or RDSP to conduct, tests.</p> <p>(g) Take any other action that the inspector considers appropriate and reasonably required for the purposes of the inspection.</p> | <ul style="list-style-type: none"> • Technical testing (penetration testing & vulnerability testing) • Red team exercises • Incident response tests • Business continuity/disaster recovery tests • Backup tests • Tabletop exercises <p>The Inspectorate is bound to have regard to any risks identified to the essential service that come under other relevant regulations including the Water Industry Act 1991, Water Supply (Water Quality) Regulations 2016, Water Supply (Water Quality) Regulations (Wales) 2016, Data Protection Act 2018, Security and Emergency Measures Direction 2024, the Civil Contingencies Act 2004, amongst others.</p> <p>The Inspectorate will endeavour to highlight any such instances at the time of finding to the OES and act in accordance with the relevant regulations/legislation.</p> |
| <p>16.—(6) The inspector must—</p> <p>(a) produce proof of the inspector's identity if requested by any person present at the premises; and</p> <p>(b) take appropriate and proportionate measures to ensure that any material, document, information or equipment removed in accordance with paragraph (5)(d) is kept secure from unauthorised access, interference and physical damage.</p> | <p>The Inspectorate and/or third-party will provide identification on request, including but not limited to:</p> <ul style="list-style-type: none"> • Inspectorate Warrant Card • Driving License • Passport • Vetting / Clearance Card or Documentation • And/or any other form of valid ID <p>There is a phone number and process that can be used to check the validity of identification, which can be provided by the Inspector.</p> <p>The Inspectorate will, in line with its data classification policies, and wider HMG data classification policies, ensure that any removed documentation is stored securely, therefore reducing the risk of interception by an unauthorised party.</p> <p>Where the Inspectorate takes equipment or forensic images for evidence purposes, utmost care will be taken to ensure the chain of custody will be maintained and that no operational impact on the essential service will occur as a consequence of confiscation.</p> |
| <p>16.—(7) Before exercising certain powers, the inspector must ensure that:</p> <p>(a) The ability of the OES to deliver essential services is not affected.</p> | <p>Inspections must be conducted carefully to ensure they do not disrupt the essential service. Where testing activity is undertaken a robust pre-testing risk assessment specific to the planned activity</p> |

| | |
|---|--|
| (b) Risks are properly assessed. | <p>must be undertaken with all entities involved undertaken at scoping, and at any other relevant planning stage.</p> <p>Inspectors and any third-party that is used on behalf of the Inspectorate will abide by water company policy and procedures when visiting sites that are restricted or require Water Hygiene Cards (EUSR) or specific Personal Protective Equipment (PPE) requirements.</p> |
| <p>16.—(8) Where under paragraph (5)(d) an inspector removes any document, material or equipment, the inspector must provide, to the extent practicable, a notice giving—</p> <p>(a)sufficient particulars of that document, material or equipment for it to be identifiable; and</p> <p>(b)details of any procedures in relation to the handling or return of the document, material or equipment.</p> | <p>As above, the Inspectorate will, in line with its data classification policies, and wider HMG data classification policies, ensure that any removed documentation is stored securely, therefore reducing the risk of interception by an unauthorised party.</p> <p>The Inspectorate will, in line with the GSCP, treat protectively marked materials in accordance with their designated handling requirements.</p> <p>The Inspectorate will ensure that all relevant staff have undertaken appropriate data handling training to manage classified materials securely and in line with the GSCP.</p> |

| Regulation | Guidance |
|---|--|
| Enforcement [notices] for breach of duties | |
| <p>17.—(1) A competent authority may serve an enforcement notice on an OES if it has reasonable grounds to believe that the OES has failed to:</p> <p>(a) fulfil the security duties under regulation 10(1) and (2);</p> <p>(b) notify a NIS incident under regulation 11(1);</p> <p>(c) comply with the notification requirements stipulated in regulation 11(3);</p> <p>(d) notify an incident as required by regulation 12(9);</p> <p>(e) comply with an information notice issued under regulation 15; or</p> <p>(f) comply with—</p> <p>(i) a direction given under regulation 16(1)(c), or</p> <p>(ii) the requirements stipulated in regulation 16(3).</p> | <p>If an OES fails to comply with the NIS Regulations, the Inspectorate can issue an enforcement notice, requiring corrective action. This may relate to:</p> <p>Failure to implement appropriate cyber security measures as required under Regulation 10(1), such as:</p> <ul style="list-style-type: none"> • Lack of adequate network segmentation to protect operational systems. • Absence of multi-factor authentication (MFA) or access controls on critical systems. • Failure to implement patching and vulnerability management processes. • Insufficient system monitoring or threat detection capabilities. • Lack of risk-based security policies and governance frameworks. <p>Failure to prevent and minimise the impact of security incidents, as required under Regulation 10(2), such as:</p> |

| | |
|---|--|
| | <ul style="list-style-type: none"> • Absence of a robust incident response plan or failure to conduct regular exercises. • Inadequate backup and disaster recovery plans, affecting service continuity. • Failure to establish business continuity measures for cyber disruptions. • Insufficient forensic logging and monitoring, limiting incident investigations. • Failure to remediate or mitigate against a recurrence of a specific incident, failing to action lessons learned from previous incidents. <p>Failure to report security incidents in line with Regulation 11(1), including:</p> <ul style="list-style-type: none"> • Not notifying the Inspectorate within 72 hours of a significant NIS-related cyber incident. • Underreporting incidents that impact service continuity or the security of the essential function. • Failure to provide an adequate post-incident report with root cause analysis. <p>Failure to provide requested information as required under Regulation 15, such as:</p> <ul style="list-style-type: none"> • Non-compliance within CAF self-assessments or audits. • Withholding penetration test reports, risk assessments, or testing schedules. • Delays in submitting progress updates on regulatory notices. |
| <p>17.—(2A) Before serving an enforcement notice under paragraph (1) or (2), the relevant competent authority or the Information Commissioner must inform the OES or RDSP, in such form and manner as it considers appropriate having regard to the facts and circumstances of the case, of—</p> <p>(a) the alleged failure; and</p> <p>(b) how and by when representations may be made in relation to the alleged failure and any related matters.</p> | <p>Before taking formal enforcement action, the Inspectorate must notify the OES of the suspected non-compliance and give them an opportunity to respond, ensuring:</p> <ul style="list-style-type: none"> • Transparency in enforcement actions. • A chance for the OES to explain or dispute allegations. • An opportunity to provide evidence of compliance or mitigating circumstances. <p>The response must be submitted within the timeframe, format and manner specified by the Inspectorate (within the DWI Network and Information Systems Enforcement Policy and a Notice of Intention letter).</p> |
| <p>17.—(2B) When the relevant competent authority or the Information Commissioner informs the OES</p> | <p>The Inspectorate can issue a formal warning before proceeding with an enforcement notice, allowing</p> |

| | |
|---|---|
| or RDSP in accordance with paragraph (2A), it may also provide notice of its intention to serve an enforcement notice. | the OES to take corrective action voluntarily. However, this step is discretionary, meaning the Inspectorate is not required to give a prior warning in all cases. This will be determined on a case-by-case basis. |
| 17.—(2C) The relevant competent authority or the Information Commissioner may serve an enforcement notice on the OES or RDSP within a reasonable time, irrespective of whether it has provided any notice in accordance with paragraph (2B), having regard to the facts and circumstances of the case, after it has informed the OES or RDSP in accordance with paragraph (2A). | The Inspectorate is not obligated to wait after issuing a warning and may proceed with an enforcement notice promptly if it determines that further regulatory action is necessary. The timeframe for issuing the enforcement notice must be reasonable, taking into account the severity and urgency of the non-compliance. |
| 17.—(2D) The relevant competent authority or the Information Commissioner must have regard to any representations made under paragraph (2A)(b). | Any responses from the OES must be considered by the Inspectorate before finalising enforcement action, which will be internally reviewed after consideration by a Deputy Chief Inspector, and/or the Chief Inspector, as appropriate. This ensures that reasonable justifications or remedial actions taken by the OES are taken into account before proceeding with penalties or further regulatory action. All enforcement activity served and proposed alike, is noted and recorded by the Inspectorate. |
| 17.—(3) An enforcement notice must: (a) State the reasons for its issuance. (b) Describe the alleged failure. (c) Outline steps to rectify the failure and deadlines. | OES' must comply with enforcement notices, addressing security deficiencies within the specified timeframe provided by the Inspectorate on issuance of the enforcement notice. Any enforcement notice served will cover these points and/or covered them within an accompanying covering letter issued by the Inspectorate. |
| 17.—(4) If the relevant competent authority or the Information Commissioner is satisfied that no further action is required, having considered: (a) Any representations submitted by the OES or RDSP. (b) Any corrective actions taken to rectify the alleged failure. It must inform the OES or RDSP in writing as soon as reasonably practicable. | If an OES provides a valid response or rectifies the issue, the Inspectorate must formally confirm in writing that no further action will be taken. The notification must be provided without unnecessary delay to close the matter efficiently. |
| 17.—(5) The OES or RDSP may request reasons for a decision to take no further action under paragraph (4) within 28 days of being informed of that decision. | If an OES wants further clarification on why no enforcement action was taken, it has 28 days to request an explanation from the Inspectorate. This may be useful if: - The OES wants confirmation of specific compliance improvements. - The OES seeks to understand regulatory expectations for future compliance. |

| | |
|--|--|
| | - The OES believes the issue may still require enhanced internal attention despite no enforcement being taken. |
| (6) Upon receipt of a request under paragraph (5), the relevant competent authority or Information Commissioner must provide written reasons for a decision under paragraph (4) within a reasonable time and in any event no later than 28 days. | If corrective action is taken, the Inspectorate will confirm compliance and close the enforcement case. |

| Regulation | Guidance |
|--|---|
| Penalties | |
| 18.—(1) The designated competent authority for an OES may serve a notice of intention to impose a penalty if it has reasonable grounds to believe the OES has failed to comply with a duty under regulation 17(1) or 17(3A), and considers a penalty is warranted having regard to the facts and circumstances of the case. | <p>The Inspectorate can issue a notice of intention to impose a financial penalty on an OES if it determines that the OES has failed to meet its duties under the NIS Regulations. This could relate to:</p> <ul style="list-style-type: none"> - Failure to implement appropriate security measures. - Failure to notify the Inspectorate incidents (in whole, in part, or within the designated timeframes). - Non-compliance with enforcement notices. <p>The Inspectorate must have reasonable grounds and must consider the facts and circumstances of the case before issuing the notice of intention to impose a penalty.</p> |
| <p>18.—(3) A notice of intention to impose a penalty must be in writing and must specify the following-</p> <ul style="list-style-type: none"> (a) the reasons for imposing a penalty; (b) the sum that is intended to be imposed as a penalty and how it is to be paid; (c) the date on which the notice of intention to impose a penalty is given; (d) the period within which a penalty will be required to be paid if a penalty notice is served. (e) that the payment of a penalty under a penalty notice (if any) is without prejudice to the requirements of any enforcement notice (if any); and (f) how and when representations may be made about the content of the notice of intention to impose a penalty and any related matters | <p>The notice of intention to impose a penalty must provide:</p> <ul style="list-style-type: none"> - Clear reasons for the penalty (detailing the breaches or failures that led to the issuance of a notice of intention to impose a financial penalty). - The proposed penalty amount and calculation of quantum. - Information on how to pay the penalty. - Confirmation that paying the penalty does not exempt the OES from fulfilling any outstanding enforcement actions, such as enforcement notices (which may be designated alongside or separately from a financial penalty). - An opportunity for the OES to submit a formal response or defence (representations) to the Inspectorate, in the form of an appeal. |
| 18.—(3A) The relevant competent authority may, after considering any representations submitted in accordance with paragraph (3)(f), serve a penalty notice on the OES with a final penalty decision if the authority is satisfied that a penalty is | <p>The Inspectorate must review any representations from the OES and take them into account before issuing a final penalty notice. This ensures:</p> <ul style="list-style-type: none"> - Fair consideration of the OES' position. |

| | |
|--|---|
| warranted having regard to the facts and circumstances of the case. | - The penalty reflects all circumstances relevant and any aggravating factors, mitigating factors or corrective actions already taken following a breach of the NIS regulations. |
| 18.—(3C) The relevant competent authority or the Information Commissioner may serve a notice of intention to impose a penalty or a penalty notice irrespective of whether it has served or is contemporaneously serving an enforcement notice on the OES or RDSP under regulation 17(1) or (2). | Penalties can be imposed by the Inspectorate independently of other enforcement action. For example, an OES could be fined for failing to report an incident, even if no enforcement notice was previously issued. A notice of intention to impose a penalty could be served where additional evidence comes to light after an enforcement notice has been served or the closing of an incident case that the Inspectorate deems sufficiently applicable to warrant a penalty. |
| <p>18.—(3D) A penalty notice must—</p> <p>(a) Be given in writing to the OES or RDSP;</p> <p>(b) Include reasons for the final penalty decision;</p> <p>(c) Require the OES or RDSP to pay—</p> <p style="padding-left: 40px;">(i) The penalty specified in the notice of intention to impose a penalty; or</p> <p style="padding-left: 40px;">(ii) Such penalty as the relevant competent authority or the Information Commissioner considers appropriate in the light of any representations made by the OES or RDSP and any steps taken by the OES or RDSP to rectify the failure or to do one or more of the things required by an enforcement notice under regulation 17(3);</p> <p>(d) Specify the period within which the penalty must be paid (“the payment period”) and the date on which the payment period is to commence;</p> <p>(e) Provide details of the appeal process under regulation 19A; and</p> <p>(f) Specify the consequences of failing to make payment within the payment period.</p> | <p>The final penalty notice is a formal document setting out:</p> <ul style="list-style-type: none"> - The outcome of the regulatory review. - The confirmed penalty amount. - The deadline for payment (the payment period). - How to appeal (see Regulation 19A). - What will happen if the fine is not paid (e.g. further enforcement action). <p>The final penalty notice will only be issued following representations from the affected OES. Final decisions are made by the Chief Inspector, and the decision is recorded in writing and kept on the OES’ record.</p> <p>The final penalty notice will outline the payment method that will be used by the OES, regulation 22 (1) outlines information regarding the Proceeds of penalties.</p> |
| 18.—(3E) It is the duty of the OES or RDSP to comply with any requirement imposed by a penalty notice. | OES’ must comply with any requirements imposed upon them through the penalty notice by the Inspectorate. For further information, please see above. |
| 18.—(4) (4) A competent authority or the Information Commissioner may withdraw a penalty notice by informing the person upon whom it was served in writing. | <p>The Inspectorate reserves the right to withdraw a penalty notice if, for example (but not limited to):</p> <ul style="list-style-type: none"> - Further evidence demonstrates the OES was compliant. |

| | |
|--|--|
| | <ul style="list-style-type: none"> -Further evidence demonstrates that the culpability of an OES has changed, in accordance with our penalty-summation methodology. - New information emerges that mitigates the original breach. - A penalty notice is not proportional to the breach. |
| <p>18.—(5) The sum [of any penalty imposed] under this regulation must be an amount that—</p> <p>(a) The competent authority or Information Commissioner determines is appropriate and proportionate to the failure in respect of which it is imposed; and</p> <p>(b) is in accordance with paragraph (6).</p> | <p>Penalties are designated at the discretion of the Inspectorate, in line with the NIS Regulations and the DWI's Network and Information Systems Regulations Enforcement Policy. The Environmental Sentencing Guidelines framework was referred to in developing the enforcement policy. Penalties must be appropriate and proportionate.</p> <p>Any financial penalties must reflect:</p> <ul style="list-style-type: none"> - The seriousness of the breach. - The culpability of the OES in its failure. - The impact on the essential service (including number of systems/customers affected, downtime, and any other impacts to the delivery of clean and safe drinking water). - Any mitigating factors (an example of, but not restricted to- voluntary improvements made by the OES). |
| <p>18.—(6) The amount must—</p> <p>(a) Not exceed £1,000,000 for any contravention which the enforcement authority determines [was not a material contravention];</p> <p>(b)</p> <p>(c) Not exceed £8,500,000 for a material contravention which the enforcement authority determines [does not meet the criteria set out in sub-paragraph (d)]; and</p> <p>(d) Not exceed £17,000,000 for a material contravention which the enforcement authority determines [has or could have created a significant risk to, or significant impact on, or in relation to, the service provision by the OES or RDSP].</p> | <p>Penalties are tiered according to the severity of non-compliance and specific circumstances warranting a penalty relating to the risk posed to the essential service or actual significant impact. The penalty tiers under the Regulations are as follows:</p> <ul style="list-style-type: none"> - Up to £1 million for contraventions, that were not deemed material. - Up to £8.5 million for more serious contraventions that were deemed material but not warranting the maximum band of penalty. - Up to £17 million for the most serious cases of material contravention. <p>Specific cases of the types of contraventions are outlined further in the published DWI Network and Information Systems Enforcement Policy.</p> |

| Regulation | Guidance |
|--|---|
| Appeal by an OES or RDSP to the First-tier Tribunal | |
| 19A.—(1) An OES may appeal to the First-tier Tribunal against one or more of the following | OES' have the legal right to challenge certain regulatory decisions made by Inspectorate by appealing to the First-tier Tribunal (General |

| | |
|--|--|
| <p>decisions made by the designated competent authority:</p> <p>(a) A decision under regulation 8(3) to designate that person as an OES.</p> <p>(b) A decision under regulation 9(1) or 9(2) to revoke the designation of that OES.</p> <p>(c) A decision under regulation 17(1) to serve an enforcement notice.</p> <p>(d) A decision under regulation 18(3A) to serve a penalty notice.</p> | <p>Regulatory Chamber). This right applies to decisions related to:</p> <ul style="list-style-type: none"> - Designation as an OES (including instances where designation is imposed despite not meeting thresholds, such as population served). - Revocation of OES status. - Issuance of enforcement notices requiring remedial action. - Issuance of penalty notices imposing financial penalties. <p>Appeals allow OES' to seek independent judicial review of the Inspectorates decisions.</p> |
| <p>19A.—(3) Grounds for appeal are:</p> <p>(a) The decision was based on a material error as to the facts.</p> <p>(b) That any of the procedural requirements under these Regulations in relation to the decision have not been complied with and the interests of the OES or RDSP have been substantially prejudiced by the non-compliance.</p> <p>(c) The decision was wrong in law.</p> <p>(d) There was some other material irrationality, including unreasonableness or lack of proportionality, which has substantially prejudiced the interests of the OES or RDSP.</p> | <p>Grounds for appeal cover factual errors, procedural unfairness, legal errors, and unreasonable decisions.</p> <p>An appeal by an OES can be lodged on several grounds. Instances where an OES can lodge an appeal could include scenarios where:</p> <ul style="list-style-type: none"> - The Inspectorate based its decision on incorrect or incomplete facts. - The Inspectorate failed to follow correct procedures, affecting the fairness of the process. - The Inspectorate misinterpreted the law. - The Inspectorates decision was unreasonable, disproportionate, or irrational to the extent that it unfairly harmed the OES. <p>OES' must clearly identify the grounds for appeal when submitting their case to the First-tier Tribunal.</p> |

| Regulation | Guidance |
|--|--|
| Decision of the First-tier Tribunal | |
| <p>19B.—(1) The First-tier Tribunal must determine the appeal after considering the grounds of appeal referred to in regulation 19A(3) and by applying the same principles as would be applied by a court on an application for judicial review.</p> | <p>The First-tier Tribunal will review the appeal based on the grounds submitted by the OES (see Regulation 19A). The Tribunal will assess whether the Inspectorates decision was made lawfully, fairly, and reasonably, using judicial review principles. This means the Tribunal will consider:</p> <ul style="list-style-type: none"> - Did the Inspectorate follow correct procedures? - Was the decision rational and based on proper evidence? |

| | |
|--|--|
| | <ul style="list-style-type: none"> - Was the law applied correctly? - Did the decision fall within the Inspectorates legal powers? <p>It is noted that the Tribunal will not conduct a full re-hearing of the case but will assess whether the Inspectorate acted properly in reaching its decision.</p> <p>First-Tier Tribunal cases and details of cases are not made available to the public.</p> |
| <p>19B.—(2) The Tribunal may, until it has determined the appeal (or the appeal is withdrawn), suspend the effect of the whole or part of any of the following decisions:</p> <ul style="list-style-type: none"> (a) Designation as an OES under regulation 8(3); (b) Revocation of OES status under regulation 9(1) or 9(2); (c) An enforcement notice under regulation 17(1) or 17(2); (d) & (e) A penalty notice under regulation 18(3A) or 18(3B). | <p>If an OES lodges an appeal, the Tribunal may pause (suspend) the legal effect of certain Inspectorate decisions whilst the appeal is ongoing. This could include suspending:</p> <ul style="list-style-type: none"> - Designation or revocation of OES status. - Enforcement notices requiring action. - Penalty notices requiring payment. <p>Suspension prevents the OES from being penalised or forced to act until the Tribunal makes a final decision. This ensures no irreversible action (such as payment of a penalty notice or changes to OES internal processes/systems) is taken before the appeal is resolved.</p> |
| <p>19B.—(3) The Tribunal may:</p> <ul style="list-style-type: none"> (a) Confirm any decision to which the appeal relates; or (b) Quash the whole or part of any decision to which the appeal relates. | <p>Following its review, the Tribunal has two main options:</p> <ul style="list-style-type: none"> - Confirm the Inspectorate’s decision, meaning the appeal is dismissed. - Quash (overturn) the Inspectorate’s decision, either in whole or in part. <p>Quashing a decision means the Inspectorate’s original action is cancelled or amended.</p> |
| <p>19B.—(4) Where the Tribunal quashes the whole or part of a decision to which the appeal relates, it must remit the matter back to the designated competent authority for the OES or, as the case may be, the Information Commissioner, with a direction to that authority or the Commissioner to reconsider the matter and make a new decision having regard to the ruling of the Tribunal.</p> | <p>If the Tribunal quashes a decision, the case is returned to the Inspectorate for reconsideration. The Inspectorate, in their role as the CA, must reassess the matter, making a new decision that follows the Tribunal’s legal findings and guidance. The Tribunal does not substitute its own decision for the Inspectorate’s decision — the Inspectorate must re-make the decision itself, but in line with the Tribunal’s directions.</p> |
| <p>19B.—(5) The relevant competent authority or, as the case may be, the Information Commissioner, must have regard to a direction under paragraph (4).</p> | <p>The Inspectorate is legally obliged to follow the Tribunal’s instructions when reconsidering the case. Failure to follow the Tribunal’s directions could lead to further legal challenge.</p> |
| <p>19B.—(6) Where the relevant competent authority or, as the case may be, the Information Commissioner, makes a new decision in accordance with a direction under paragraph (4), that decision is to be considered final.</p> | <p>Once the Inspectorate makes its revised decision, following a Tribunal ruling, the new decision is final. This concludes the process, unless the OES challenges the new decision through further legal action (such as judicial review in a higher court).</p> |

| Regulation | Guidance |
|---|---|
| Enforcement by civil proceedings | |
| A20.—(1) This regulation applies where— (a) The designated competent authority for an OES has reasonable grounds to believe that the OES has failed to comply with the requirements of an enforcement notice under regulation 17(3A); or (b) The Information Commissioner has reasonable grounds to believe that a RDSP has failed to comply with the requirements of an enforcement notice under regulation 17(3A). | If an OES fails to comply with the terms of an enforcement notice issued by the Inspectorate, the Inspectorate has the option to take formal legal action through the civil courts. This provides the Inspectorate with a legal mechanism to compel compliance where enforcement notices are ignored or inadequately actioned, specifically petitioning the courts for a court order. |
| A20.—(2) This regulation applies irrespective of whether the OES or RDSP has appealed to the First-tier Tribunal under regulation 19A. | Even if an OES has lodged an appeal to the First-Tier Tribunal, the Inspectorate may still initiate civil proceedings if the OES fails to comply with the enforcement notice. However, this is subject to restrictions in paragraph (3). |
| A20.—(3) But where an OES or RDSP has appealed to the First-tier Tribunal under regulation 19A and the Tribunal has granted a suspension of the effect of the whole or part of the relevant decision under regulation 19B(2), the relevant competent authority or the Information Commissioner, as the case may be, may not bring or continue proceedings under this regulation in respect of that decision or that part of that decision for as long as the suspension has effect. | As per 19B(2), if the Tribunal has ‘paused’ (suspended) the enforcement notice, the Inspectorate cannot proceed with civil enforcement until the Tribunal reaches its decision and the suspension ends. This ensures that ongoing appeals are respected, and enforcement action is not prematurely escalated. |
| A20.—(4) Where paragraph (1)(a) applies, the relevant competent authority may commence civil proceedings against the OES— (a) For an injunction to enforce the duty in regulation 17(3A); (b) For specific performance of a statutory duty under section 45 of the Court of Session Act 1988; or (c) For any other appropriate remedy or relief. | If an OES ignores or fails to comply with an enforcement notice, the Inspectorate can apply to the civil courts for legal remedies, including: - An injunction to legally compel the OES to comply with its duties. - A specific court order, which legally requires the OES to take the actions set out in the enforcement notice. - Any other legal remedy the court considers appropriate, such as a declaratory judgement or other legally binding order. This provides the Inspectorate with a direct legal route to force action from an OES regarding NIS compliance if previous formal measures have failed, failure to abide by a court order would place an OES in contempt of court. |
| A20.—(6) No civil proceedings may be commenced under this regulation before the end of a period of 28 days beginning with the day on which the last relevant enforcement notice was served on the OES or, as the case may be, RDSP. | The Inspectorate must wait at least 28 days after serving the enforcement notice before starting civil proceedings, allowing the OES time to respond or rectify the breach. |

| | |
|---|---|
| A20.—(7) In this regulation, a reference to civil proceedings is a reference to proceedings, other than proceedings in respect of an offence, before a civil court in the United Kingdom. | This confirms that these enforcement actions are civil (regulatory) matters, not criminal prosecutions. They will be heard in the civil courts (High Court or County Court), depending on the circumstances, and dependent on which track the case is referred to. |
|---|---|

| Regulation | Guidance |
|--|--|
| Enforcement of penalty notices | |
| 20.—(1) This paragraph applies where a sum is payable to an enforcement authority as a penalty under regulation 18. | Where an OES has been issued a penalty notice under Regulation 18, and the penalty has not been paid within the required period, the Inspectorate has the power to recover the penalty through the courts. This regulation sets out the legal mechanisms for recovering unpaid penalties. |
| 20.—(2) In England and Wales, the penalty is recoverable as if it were payable under an order of the county court or of the High Court. | In England and Wales, the Inspectorate can apply to either a County Court or the High Court to recover the unpaid penalty. The court treats the penalty as if it were a court-ordered debt, meaning the Inspectorate can use court enforcement methods to recover the sum. |
| 20.—(5) Where action is taken under this paragraph for the recovery of a sum payable as a penalty under regulation 18, the penalty is — (a) In England and Wales, to be treated for the purposes of section 98 of the Courts Act 2003 as if it were a judgment entered in the county court. | This section ensures that penalties are treated as enforceable court judgments in both England and Wales and Northern Ireland. This allows the Inspectorate to use the same enforcement tools available to creditors, including: - Warrants of control (bailiff action) - Third party debt orders (freezing bank accounts) |
| 20.—(6) No action may be taken under this paragraph for the recovery of a sum payable as a penalty under regulation 18 if an appeal has been brought under regulation 19A and the appeal has not been determined or withdrawn. | If the OES appeals the penalty notice to the First-tier Tribunal (under Regulation 19A), the Inspectorate cannot begin court proceedings to recover the penalty until the appeal is resolved. This protects OES from enforcement action whilst the appeal process is ongoing. |

Part 6: Miscellaneous

| Regulation | Guidance |
|--|--|
| Fees | |
| 21.—(1) A fee is payable by an OES or a RDSP to an enforcement authority, to recover the reasonable costs incurred by, or on behalf of, that authority in carrying out a NIS function in relation to that OES or RDSP. | OES' are required to pay fees to the Inspectorate to cover the costs associated with regulatory activities under the NIS Regulations. These costs may include inspections, audits, assessments, and compliance monitoring undertaken by or on behalf of the Inspectorate (as per 16 (1)). The fees must be reasonable and proportionate to the work carried out. |
| 21.—(2) The fee mentioned in paragraph (1) must be paid to the enforcement authority within 30 days after receipt of the invoice sent by the authority. | OES' must pay the invoiced fees within 30 days of receiving the invoice from the Inspectorate. Timely payment is required to avoid potential enforcement action. |
| 21.—(3) The invoice must state the work done and the reasonable costs incurred by, or on behalf of, the enforcement authority, including the time period to which the invoice relates. | The Inspectorate must provide a clear breakdown of the work performed and associated costs when issuing an invoice. This ensures transparency in the charging of fees and allows OES' to understand the basis of the charges incurred. |
| 21.—(4) An enforcement authority may determine not to charge a fee under paragraph (1) in any particular case. | The Inspectorate has discretion to waive or reduce fees in specific cases. This may apply where minimal regulatory intervention was required or in exceptional circumstances where charging a fee would be disproportionate. |
| 21.—(5) A fee payable under this regulation is recoverable as a civil debt. | Unpaid fees can be recovered through civil court proceedings. If an OES fails to pay, the Inspectorate can pursue legal action to recover the outstanding amount as a debt. |
| 21.—(6) In this regulation— (a) a “NIS function” means a function that is carried out under these Regulations except any function under regulations 17(1) to (4) and 18 to 20; and (b) “enforcement authority” has the same meaning as in regulation 18(7)(b). | NIS functions for which fees are charged include routine regulatory activities such as inspections, audits, assessments, compliance reviews, and guidance issuance. |

| Regulation | Guidance |
|--|---|
| Proceeds of penalties | |
| 22.—(1) The sum that is received by a NIS enforcement authority as a result of a penalty notice served under regulation 18 must be paid into the Consolidated Fund unless paragraph (2) applies. | Any financial penalties collected by Inspectorate under Regulation 18 are not retained by the enforcement authority but must be paid into the UK Government's Consolidated Fund. The Consolidated Fund is the Government's main account for public revenue, meaning penalty payments contribute to general government |

| | |
|---|--|
| | expenditure rather than funding the Inspectorate's regulatory activities. |
| 22.—(2) The sum that is received as a result of a penalty notice served under regulation 18 by— (a) the Welsh Ministers must be paid into the Welsh Consolidated Fund established under section 117 of the Government of Wales Act 2006; and (b) the Scottish Ministers or the Drinking Water Quality Regulator for Scotland, must be paid into the Scottish Consolidated Fund established under section 64 of the Scotland Act 1998. | <p>If a penalty is issued in Wales, the proceeds are directed to the respective devolved government funds.</p> <p>Penalties collected by the Welsh Ministers under NIS enforcement must be paid into the Welsh Consolidated Fund, which finances the Welsh Government's public services.</p> <p>This ensures that penalties collected under the NIS Regulations in devolved administrations remain within their respective financial systems rather than being transferred to the UK-wide Consolidated Fund.</p> |

| Regulation | Guidance |
|---|---|
| Enforcement action – general considerations | |
| 23.—(1) Before a NIS enforcement authority takes any action under regulation [17 (1) or (2), 18(3A) or (3B) or A20,] the enforcement authority must consider whether it is reasonable and proportionate, on the facts and circumstances of the case, to take action in relation to the contravention. | <p>The Inspectorate must ensure that any enforcement action taken against an OES is reasonable and proportionate. This means that the Inspectorate must assess the specific facts of the case before issuing:</p> <ul style="list-style-type: none"> - An enforcement notice (Regulation 17) - A penalty notice (Regulation 18) - Civil enforcement proceedings (Regulation A20) <p>This prevents unfair or excessive enforcement and ensures that regulatory action is justified and appropriate to the circumstances.</p> |
| 23.—(2) The NIS enforcement authority must, in particular, have regard to the following matters— (a) Any representations made by the OES or RDSP, as the case may be, about the contravention and the reasons for it, if any; (b) Any steps taken by the OES or RDSP to comply with the requirements set out in these Regulations; (c) Any steps taken by the OES or RDSP to rectify the contravention; (d) Whether the OES or RDSP had sufficient time to comply with the requirements set out in these Regulations; (e) Whether the contravention is also liable to enforcement under another enactment. | <p>When determining whether enforcement action is necessary and proportionate, the Inspectorate must consider key factors before making a decision. These factors ensure that OES' are treated fairly and given a reasonable opportunity to comply.</p> <ul style="list-style-type: none"> - OES' must be given the opportunity to make representations before enforcement action is taken. The Inspectorate must consider any explanations provided, including mitigating circumstances or external factors that contributed to the non-compliance. - If an OES has already taken corrective action or is in the process of complying with the NIS Regulations, the Inspectorate must take this into |

| | |
|--|--|
| | <p>account when deciding whether further enforcement is necessary.</p> <ul style="list-style-type: none"> - The Inspectorate must assess the OES' response to the issue. If the OES has already fixed the problem, the need for enforcement action may be reduced or eliminated. - The Inspectorate must ensure that OES' have had a reasonable amount of time to comply before taking enforcement action. If compliance was expected within an unrealistic timeframe, this may be a reason to delay enforcement action. - If the same issue is being investigated under a different law or regulations (e.g. under environmental, health and safety, or data protection laws), the Inspectorate must consider whether additional enforcement under the NIS Regulations is necessary or appropriate. This will typically be decided by a Deputy Chief Inspector or Chief Inspector. |
|--|--|

| Regulation | Guidance |
|--|---|
| Service of documents | |
| <p>24.—(1) Any document or notice required or authorised by these Regulations to be served on a person may be served by—</p> <ul style="list-style-type: none"> (a) delivering it to that person in person; (b) leaving it at the person's proper address; or (c) sending it by post or electronic means to that person's proper address. | <p>Formal notices and documents issued under the NIS Regulations, including enforcement notices, penalty notices, and information notices, must be properly served to ensure they are legally valid.</p> <p>OES' must ensure they have a designated contact point for regulatory correspondence to avoid missing important notifications. Documents can be served:</p> <ul style="list-style-type: none"> - In person to the recipient. - Left at the recipient's proper address. - Sent via post or by email to an official address. <p>Email is the Inspectorate's preferred delivery method; the Inspectorate will typically request confirmation of receipt from the recipient on behalf of the OES.</p> |
| <p>24.—(2) In the case of a body corporate, a document may be served on a director of that body.</p> | <p>If an OES is a corporate entity, the Inspectorate can serve documents directly to a company director, ensuring that senior leadership is aware of regulatory actions. Designated Board-level NIS contacts will be served any such documents.</p> |
| <p>24.—(3) In the case of a partnership, a document may be served on a partner or person having control or management of the partnership business.</p> | <p>If an OES operates as a partnership, documents may be served on:</p> <ul style="list-style-type: none"> - A named partner of the business. - Any person responsible for managing the partnership. |

| | |
|--|--|
| 24.—(4) If a person has specified an address in the United Kingdom (other than that person's proper address) at which that person or someone on that person's behalf will accept service, that address must also be treated as that person's proper address. | If an OES designates an alternative address (e.g. a legal representative's office), official notices can be legally served at that address instead of the company's main registered office. |
| 24.—(5) For the purposes of this regulation "proper address" means— (a) in the case of a body corporate or its director— (i) the registered or principal office of that body; or (ii) the email address of the secretary or clerk of that body; (b) in the case of a partnership, a partner or person having control or management of the partnership business— (i) the principal office of the partnership; or (ii) the email address of a partner or a person having that control or management; (c) in any other case, a person's last known address, which includes an email address. | The proper address for service depends on the type of entity: - For corporations: Notices should be sent to the registered office or the email of a company secretary or clerk. - For partnerships: The main business office or a partner's email can be used. - For individuals: The last known physical or email address is valid for service. As per 8A.—(3), OES' must ensure their contact details are up to date with the Inspectorate to avoid missing important regulatory communications. |

| Regulation | Guidance |
|---|---|
| Review and report | |
| 25.—(1) The Secretary of State must— (a) carry out a review of the regulatory provision contained in these Regulations [in EU Regulation 2018/151]; and (b) publish a report setting out the conclusions of that review. | The Secretary of State is responsible for periodically reviewing the effectiveness of the NIS Regulations and the related EU Regulation 2018/151 (which specifies security measures for Digital Service Providers). This review ensures that the regulations remain effective, relevant, and appropriate for managing cyber and operational resilience in critical services such as water supply. The findings of this review must be published in an official report to provide transparency and accountability on how well the regulations are achieving their objectives. |
| 25.—(2) The first report must be published on or before 9th May 2020 [F134, the second report must be published on or before 9th May 2022] and subsequent reports must be published at [F135 intervals not exceeding five years]. | Reports on the effectiveness of the NIS Regulations must be published at least every five years. This ensures that the legal framework remains up to date with evolving cyber threats, technological advancements, and changes in operational security risks. OES' should monitor these reports as they may lead to updates in compliance expectations or changes to enforcement priorities. |

| | |
|--|--|
| <p>25.—(4) Section 30(4) of [the Small Business, Enterprise and Employment Act 2015] requires that reports published under this regulation must, in particular—</p> <p>(a) set out the objectives intended to be achieved by the regulatory provision referred to in paragraph (1)(a);</p> <p>(b) assess the extent to which those objectives are achieved;</p> <p>(c) assess whether those objectives remain appropriate; and</p> <p>(d) if those objectives remain appropriate, assess the extent to which they could be achieved in another way which involves less onerous regulatory provision.</p> | <p>The review process is structured to ensure continual improvement of the NIS Regulations by assessing:</p> <ul style="list-style-type: none"> - The original goals of the regulations. - Whether those goals are being met. - Whether the objectives are still relevant given changes in cyber threats and technology. - Whether a less burdensome regulatory approach could achieve the same objectives. <p>This process ensures that the regulatory framework remains proportionate and effective, avoiding unnecessary administrative burdens for OES’.</p> |
| <p>25.—(5) In this regulation “regulatory provision” has the same meaning as in sections 28 to 32 of that Act.</p> | <p>This regulation aligns with wider UK Government requirements for reviewing and assessing the impact of regulations on businesses and public services under the Small Business, Enterprise and Employment Act 2015.</p> |

Annex A: Schedule 1: Designated Competent Authorities

| Relevant Sectors | Subsectors | Designated Competent Authorities |
|------------------|---|---|
| Energy | Electricity | The Secretary of State for Energy Security and Net Zero (England and Wales and Scotland) and the Gas and Electricity Markets Authority (acting jointly). The Department of Finance (Northern Ireland) |
| | Oil | The Secretary of State for Energy Security and Net Zero (England and Wales and Scotland) |
| | Gas | The Secretary of State for Energy Security and Net Zero for the essential services specified in Schedule 2, paragraph 3, subparagraphs (5) to (8) (England and Wales and Scotland). Otherwise, the Secretary of State for Energy Security and Net Zero and The Gas and Electricity Markets Authority (acting jointly). The Department of Finance (Northern Ireland) |
| Transport | Air Transport | The Secretary of State for Transport and The Civil Aviation Authority (acting jointly) (United Kingdom). |
| | Rail Transport | The Secretary of State for Transport (England and Wales and Scotland) The Department of Finance (Northern Ireland) |
| | Water Transport | The Secretary of State for Transport (United Kingdom) |
| | Road Transport | The Secretary of State for Transport (England and Wales) The Scottish Ministers (Scotland) The Department of Finance (Northern Ireland) |
| Health Sector | Health care settings (including hospitals, private clinics and online settings) | The Secretary of State for Health (England) The Welsh Ministers (Wales) The Scottish Ministers (Scotland) The Department of Finance (Northern Ireland) |

| Relevant Sectors | Subsectors | Designated Competent Authorities |
|--|--|---|
| Drinking water supply and distribution | Drinking water supply and distribution | <p>The Secretary of State for Environment, Food and Rural Affairs (England) – responsibilities are devolved to the Drinking Water Inspectorate.</p> <p>The Welsh Ministers (Wales) – responsibilities are devolved to the Drinking Water Inspectorate.</p> <p>The Drinking Water Quality Regulator (Scotland)</p> <p>The Department of Finance (Northern Ireland)</p> |
| Digital Infrastructure | Digital Infrastructure | Office of Communications (United Kingdom) |

Annex B: Schedule 2: Essential Services and Threshold Requirements

| Regulation | Guidance |
|--|---|
| Essential Services and Threshold Requirements (The drinking water supply and distribution subsector) | |
| 9. The threshold requirement which applies to the essential service of the supply of potable water in the United Kingdom is the supply of water to 200,000 or more people. | <p>Under the NIS Regulations, a water company is classified as an OES if it supplies potable (drinking) water to 200,000 or more people. This designation means the company is legally required to:</p> <ul style="list-style-type: none"> - Implement appropriate security measures to protect its network and information systems from cyber threats, physical disruptions, and other security risks. - Comply with the CAF to assess and enhance its security posture. - Report significant incidents that affect the continuity of water supply or security of its network and information systems. <p>This threshold ensures that only large-scale water providers - whose failure could have serious societal or economic consequences - are subject to these regulatory requirements.</p> |