Department
for Environment
Food & Rural Affairs

Seacole Building
4th Floor
2 Marsham Street
London
SW1P 4DF

T: 03459 33 55 77
helpline@defra.gov.uk
www.gov.uk/defra

[Redacted]
By email: [Redacted]

Our ref: FOI2024/09861
31 May 2024

Dear [Redacted] ,

REQUEST FOR INFORMATION: Network and Information Systems (NIS) Regulations 2018

Thank you for your request for information of 6 May 2024 about Network and Information Systems (NIS) Regulations 2018. We have handled your request under the Freedom of Information Act 2000 (FOIA).

Your information request and our response are set out below.

1. *The number or volume of reports of cyber security or information security incidents or breaches (i.e., "NIS Incidents" as defined in the Regulations) that have been reported to the DEFRA by regulated entities, per annum for the five years to date.*

Some of the information you have requested for the years 2023, 2022 and 2021 can be viewed here:

https://www.gov.uk/government/publications/network-and-information-systems-regulations-2018-foi202406092

As the information is reasonably accessible to you by other means, section 21 of the FOIA exempts Defra from providing a copy of the information with this response to your request.

The numbers of NIS Incidents for 2019 and 2020 are given in the following table per annum. The following table and the table in the link above give the number reported for the last five years to date, as stipulated in the request for Operators of Essential Services (OESs) in England (regulated entities under NIS).

	2019	**2020**
Reported NIS incidents	2	0
Other Incidents below threshold for NIS	2	3

We have considered the classification of reporting under the NIS Regulations to Drinking Water Inspectorate (DWI) and internally class incidents with the following criteria:

1. Cyber:- suspected or actual malicious activity on a network or information system that directly impacts on the production and delivery of wholesome water, irrespective of whether or not customers are directly affected.
2. Resilience:- A non-malicious, operational failure of a network or information system, including due to operator error or system misconfiguration, that directly impacts on the production and delivery of wholesome water which leads to a direct effect on customers.
3. Additional reporting criteria introduced for 2022, iterate that we expect companies to inform us of incidents that do not directly result in a significant impact, but nonetheless pose a risk to the security and resilience of networks and the essential services provided. (And the reason for an elevated 2022 number)

Categories 1 and 2 may be considered as a NIS Incident and category 3 as a voluntary notification. It should be understood that any notifications are interpretive both by the reporting companies and DWI and we have attempted to standardise the criteria which has produced the table above. Investigations may reveal elements that lead to a reclassification of an incident in terms of threshold reported under.

2. *The number of volume of regulatory investigations that have commenced by the DEFRA into cyber security or information security incidents or breaches (i.e., "NIS Incidents"), per annum for the five years to date.*

The DWI receives incident reports submitted under the NIS Regulations and determines what appropriate and proportionate regulatory action is required (which we class as an investigation, which would therefore include all incidents above). DWI could decide that enforcement is required or not relating to the specific circumstances of the incident. OESs are asked and expected to report the root cause and provide short-, medium- and long-term actions to rectify and resume normal operation and prevent a recurrence in 20-days post-incident reports. In addition, where water supply or distribution is impacted by any ‘event’ (which can include cyber security/NIS or resilience causes), a separate notification is reported to DWI which is investigated under the existing Water Quality Regulations.

3. *The number or volume of regulatory enforcement actions taken or imposed by the DEFRA for cyber security or information security incidents or breaches per annum for the five years to date, broken down by enforcement action type (e.g., words of advice, reprimands, changes to licence conditions, fines).*

The Drinking Water Inspectorate have initiated formal enforcement action once post-incident in 2021 under Regulation 16 (Inspection).

For one incident in 2022, the Inspectorate have served a penalty notice on the OES under Regulation 18 in addition to an Information Notice under Regulation 15 for the same incident.

We are currently investigating incidents across 2023 and 2024, no regulatory actions have been initiated to date although this may or may not change as investigations progress and are concluded.

Information disclosed in response to this FOIA request is releasable to the public. In keeping with the spirit and effect of the FOIA and the government's Transparency Agenda, this letter and the information disclosed to you may be placed on GOV.UK, together with any related information that will provide a key to its wider context. No information identifying you will be placed on the GOV.UK website.

We attach Annex A, explaining the copyright that applies to the information being released to you, and Annex B giving contact details should you be unhappy with the service you have received.

If you have any queries about this letter please contact me.

Yours sincerely

Information Rights Team
InformationRequests@defra.gov.uk

Annex A

Copyright

The information supplied to you continues to be protected by copyright. You are free to use it for your own purposes, including for private study and non-commercial research, and for any other purpose authorised by an exception in current copyright law. Documents (except photographs or logos) can be also used in the UK without requiring permission for the purposes of news reporting. Any other re-use, for example commercial publication, would require the permission of the copyright holder.

Most documents produced by Defra will be protected by Crown Copyright. Most Crown copyright information can be re-used under the Open Government Licence. For information about the OGL and about re-using Crown Copyright information please see The National Archives website.

Copyright in other documents may rest with a third party. For information about obtaining permission from a third party see the Intellectual Property Office's website.

Annex B

Complaints

If you are unhappy with the service you have received in relation to your request you may make a complaint or appeal against our decision under section 17(7) of the FOIA or under regulation 11 of the EIRs, as applicable, within 40 working days of the date of this letter. Please write to [Redacted], Head of Information Rights via email at InformationRequests@defra.gov.uk and he will arrange for an internal review of your case. Details of Defra's complaints procedure are on our website.

If you are not content with the outcome of the internal review, section 50 of the FOIA and regulation 18 of the EIRs gives you the right to apply directly to the Information Commissioner's Office (ICO) for a decision. Please note that generally the ICO cannot make a decision unless you have first exhausted Defra's own complaints procedure.

The ICO can be contacted using the following link:

https://ico.org.uk/make-a-complaint/official-information-concerns-report/official-information-concern/