Welsh Parliament
Climate Change, Environment, and Infrastructure Committee

Report on the Legislative Consent Memorandum for the Cyber Security and Resilience (Network and Information Systems) Bill

February 2026

1. The Cyber Security and Resilience (Network and Information Systems) Bill

1. The Cyber Security and Resilience (Network and Information Systems) Bill ("the Bill") was introduced in the House of Commons on 12 November 2025. The Bill is sponsored by the Department for Science, Innovation and Technology.

2. The long title of the Bill states that it is a Bill to:

> *"Make provision, including provision amending the Network and Information Systems Regulations 2018, about the security and resilience of network and information systems used or relied on in connection with the carrying on of essential activities."*[1]

[1] UK Parliament, Cyber Security and Resilience (Network and Information Systems) Bill

3. The Bill makes updates to the UK's only cross-sector cyber regulations, the Network and Information Systems Regulations 2018 (S.I. 2018/506) ("NIS Regulations"), as well as delivering new powers with the aim of ensuring government can respond to new and emerging cyber threats.

4. The NIS Regulations came into effect on 10 May 2018 and seek to ensure that essential services have adequate data and cyber security measures in place.

5. The NIS Regulations currently apply to five sectors of critical national infrastructure: transport, energy, drinking water, health and digital infrastructure, as well as some digital services including online marketplaces, search engines and cloud computing services.

6. The Bill will update the NIS Regulations by bringing more entities into their scope and equipping regulators with powers with the aim of better fulfilling their duties. The Bill includes powers to amend and add to the NIS Regulations in the future and respond to imminent and actual threats to UK national security. These reforms are intended to better protect the services and other activities that are essential to the day-to-day functioning of society in the UK, and the economy, through safeguarding relevant network and information systems (the systems that allow computers and other devices to communicate with each other) and their surrounding environment.

7. 12 regulators oversee the enforcement of the NIC Regulations. The Welsh Ministers are the designated competent authority ("DCA") for health services and for drinking water supply and distribution in Wales.

8. The Bill will modify the functions of the Welsh Minister in their role as regulator, including with new powers to designate critical supplies, expanded powers relating to enforcement, charging and information sharing. There will also be duties to issue guidance, reporting obligations and a requirement to align with the Secretary of State's strategic priorities.

9. The Welsh Ministers have delegated the majority of their functions in relation to drinking water to the Drinking Water Inspectorate ("DWI").

2. The Legislative Consent Memorandum

10. Standing Order 29.1 provides that the Welsh Ministers must lay a Legislative Consent Memorandum ("LCM") where a UK Bill makes provision "in relation to Wales that has regard to devolved matters."[2]

11. Julie James MS, Counsel General and Minister for Delivery, laid a Legislative Consent Memorandum ("the LCM") on 25 November 2025.[3]

12. The Business Committee referred the LCM to the Climate Change, Environment, and Infrastructure Committee ("the Committee") and the Legislation, Justice and Constitution Committee for consideration with a reporting deadline of 13 February 2026.[4][5]

Provisions in the Bill for which consent is sought in the LCM

13. The UK Government believes that consent is required in relation to clauses 12, 17, 19, 20, 21, 22, 29, 31, 32, 33, 34, 35, 45, 48, 49 and 50 and 51.

14. The Welsh Government agrees with this assessment but believes that consent is also required for clauses 15, 18, 25, 27, 28, 30, 36, 38, 39, 40, 41, 46, 47, 52 and 56.

Clause 12

15. Clause 12 amends the NIS Regulations to insert a new Part 4B, which provides a framework for the designation, regulation and oversight of "critical suppliers". These are suppliers of goods or services to operators of essential services ("OESs"), relevant digital service providers ("RDSPs") or Relevant Managed Service Providers ("RMSPs"), where the supplier relies on network and information systems for the purposes of that supply and an incident affecting those network and information systems could cause disruption to the essential, digital or managed services supplied to the OES, RDSP or RMSP (or essential, digital or managed services generally), and that disruption is likely to have a significant

[2] Welsh Parliament, Standing Orders of the Welsh Parliament, January 2026
[3] Welsh Government, Legislative Consent Memorandum on the Cyber Security and Resilience (Network and Information Systems) Bill
[4] Welsh Parliament, Timetable for consideration: Legislation Consent Memorandum on the Cyber Security and Resilience (Network and Information Systems) Bill, December 2025
[5] Welsh Parliament, Timetable for consideration: Legislation Consent Memorandum on the Cyber Security and Resilience (Network and Information Systems) Bill

impact on the economy or day-to-day functioning of society in all or part of the UK.

Clause 15

16. Clause 15 amends the requirements for reporting incidents in the NIS Regulations.

Clauses 17 - 22

17. Clause 17 amends the NIS Regulations related to the ability of regulators to impose charges to cover the full cost of their regulatory duties. It inserts a new Part 5A into the NIS Regulations to provide a framework for regulators to impose charges on regulated persons and/or recover costs from them, where the costs and fees relate to the discharge of their regulatory duties under the NIS Regulations. New Part 5A is inserted after regulation 20 and comprises new regulations 20A, 20B, and 20C. Regulation 21 of the NIS Regulations is omitted.

18. Clause 18 amends information sharing provisions under the NIS Regulations to create new information sharing gateways and improve safeguards on how information can be used once it has been shared under the regulations. It specifies conditions and safeguards, entities involved, and the purposes for which information may be shared.

19. Clause 19 amends the NIS Regulations to mandate that regulators publish guidance on the security requirements and incident reporting requirements for OES, RDSPs and RMSPs and for registering with the Information Commission for RDSPs and RMSPs.

20. Clause 20 amends the NIS Regulations with regards to information requirements.

21. Clause 21 amends the enforcement mechanisms available to regulators to enforce the NIS Regulations. It makes changes to the maximum amount of a penalty, the structure of the penalty banding, and other changes considered to be necessary to operationalise and improve the penalty enforcement process.

22. Clause 22 sets out that Schedule 1 contains further amendments to the enforcement and appeals provisions of the NIS Regulations.

Clause 25

23. Clause 25 makes provision about a statement of strategic priorities. Subsections (1) and (2) of this clause introduce a power for the Secretary of State to designate a statement of the UK government's strategic priorities in relation to the security and resilience of network and information systems relevant to the carrying on of essential activities. It adds that, alongside priorities, the statement must set objectives for regulators relating to the priorities and must set out the roles and responsibilities of different organisations in relation to the priorities. The power is similar to existing powers to issue statements of strategic priorities that the Secretary of State has in the Online Safety Act 2023 and the Communications Act 2003.

24. Subsection (3) requires that the designated statement must be published in a manner that the Secretary of State considers appropriate.

25. Subsection (4) establishes that a designated statement can be amended, including by being replaced in full. Subsection (5) states that a statement designated under subsection (1) may be withdrawn by the Secretary of State. Subsection (6) clarifies that a statement cannot be withdrawn or amended within three years of it having been designated, unless the criteria set out in subsection (7) are met.

26. Subsection (7) says that an amendment to, or withdrawal of, a statement can be made sooner than three years after its designation if there has been a general election, or if the Secretary of State considers that there has been a significant change in government policy or threat landscape in relation to the security and resilience of network and information systems relied on in connection with the carrying on of essential activities. Subsection (8) states that corrections to the drafting of the statement, such as to correct misspellings of words, can be made without it constituting an amendment to the designated statement

Clauses 27 - 36

27. Clause 27 introduces requirements on regulators in relation to the designated statement of strategic priorities.

28. Clause 28 sets out the reporting requirements for a Statement of Strategic Priorities issued by the Secretary of State.

29. Clause 29 makes provision about regulations relating to security and resilience of network and information systems.

30. Subsection (1) of clause 29 grants the Secretary of State powers to make regulations which can add to, amend or replace the existing NIS Regulations. It specifies that regulations can be made with the objective of identifying, managing and reducing the risks, and mitigating the adverse impacts of security or operational compromises to network and information systems (including actions related to remediation). Subsection (2) sets that that the objectives in subsection (1) may include provision for strengthening the resilience of networks and information systems, including their physical environments. Subsections (3) and (4) defines a "relevant" network and information system for the purposes of Chapter 3 of the Bill, with further explanation given for when a system is considered "associated" with another. Subsection (5) and (6) clarify what is meant by the terms "security or operational compromise," and "service-critical supply" within the Chapter.

31. Clause 30 relates to the imposition of requirements on regulated persons.

32. Subsection (1) of clause 30 expands on the extent of the power for the Secretary of State to make regulations for the purpose of protecting network and information systems, providing that regulations made under clause 29(1) can impose requirements on regulated persons. The following subsections give further detail to what requirements the regulations made under clause 29(1) can impose on regulated persons.

33. Subsection (2) and (3) defines "regulated persons" for the purposes of Chapter 3. A regulated person is a person specified, or of a description specified, for the purposes of subsection (2) in regulations made by the Secretary of State. A person (or description) may only be specified in regulations if the person (or every person of the description) carries on an essential activity in the UK or provides an activity-crucial supply. A description of persons carrying on an essential activity could, for example, be all persons carrying on that activity or a sub-set of such persons. Subsection (4) clarifies that the specification of a person or description of persons under subsection (2) can be framed by reference to whether that person or description of persons is for the time-being designated by a regulator in accordance with regulations made under clause 29(1). For example, regulations made by virtue of subsection (2) could specify as "regulated persons" any person carry on a specific type of essential activity and who is for the time-being designated by a particular regulator in accordance with regulatory provision made under clause 29. In this case, the regulator's designation decision would determine whether a particular person was subject to regulation as a "regulated person". Subsection (5) clarifies that OESs, RDSPs, RMSPs and critical suppliers are

treated as 'regulated persons' for the purposes of subsection (2). Subsection (6) provides a non-exhaustive list of specific requirements that may be imposed on regulated persons. It provides that such duties can include taking specified measures aimed at achieving objectives related to reducing and mitigating cyber security risks and impacts, as established by clause 29(1), including measures outside the UK as well as requirements in the form of prohibitions or restrictions. Additionally, it may encompass requirements regarding the reporting of certain matters, disclosing information to regulators and other persons, and appointing representatives within the UK (in the case of regulated persons established outside the UK). Subsection (7) outlines that "specified" means specified in regulations under clause 29(1).

34. Clause 31 also expands on the power for the Secretary of State to make regulations for the purpose of protecting network and information systems, setting out that the regulations made under clause 29(1) may confer functions on regulators in connection with compliance with the regulations.

35. Clause 32 sets out what can be included in regulations about financial penalties made under clause 29(1).

36. Clause 33 makes provision about the disclosure of information, guidance, the keeping of records, the preparation of reports and other matters. Clause 33(1) sets out that regulations may give functions to regulators in relation to disclosure of information, production of guidance and reports, keeping records and the consultation and cooperation with other bodies (including persons outside the UK). Subsection (2) adds more detail about what may be included in regulations made under subsection (1)(a) about the disclosure of information. Subsection (3) clarifies that the regulations may provide for information processed in accordance with regulations not to be in breach of any obligation of confidence owed by the person processing the information, or any other restrictions. Subsection (4) qualifies subsection (3), with the effect that regulations made under clause 29(1) requiring or authorising the disclosure of information cannot overrule certain prohibitions on disclosure contained in the Investigatory Powers Act 2016. Subsection (5) sets out that the regulations may place functions on persons who exercise public functions but are not regulators. This could include, for example, conferring additional functions on these authorities. Subsection (6) provides a non-exhaustive list of what these functions could entail.

37. Clause 34 makes provision about the recovery of costs of regulatory authorities. Clause 34(1) sets out that the regulations can enable regulators to impose charges on regulated persons in order to fund their functions under the

Regulations. Subsection (2) defines "relevant costs" as any costs incurred by regulators from carrying out their functions conferred by Part 3 or Part 4, or under the NIS Regulations, including costs in connection with enforcing the requirements imposed with those regulations. Subsection (3) provides that regulations may provide for the imposition of charges in accordance with a scheme made by the authority (a "charging scheme"). Subsection (4) clarifies what may be included in provisions made by regulations under subsection (1), or in charging schemes authorised by those regulations. Subsection (5) enables the regulations, or charging schemes authorised by the regulations, to impose charges (or the amount of such charges) on a person that are not limited to the costs associated with the regulation of that particular person. Subsection (6) establishes that provisions made under subsection (4)(c) may include provision about deficits incurred by a regulatory authority. Subsection (7) allows regulations made under subsection (1) to authorise a charging scheme to make different provisions for different purposes. Subsection (8) confirms the meaning of 'relevant requirement' is the same as in clause 31.

38. Clause 35 adds supplementary detail on what regulations made under clause 29(1) may do. 203. Subsection (2) makes definitions for the purposes of the Chapter.

39. Clause 36 sets out that the Secretary of State may issue a code of practice for regulated persons describing steps recommended to enable compliance with duties, requirements imposed on them, including under regulations made under clause 29(1) or the NIS Regulations. Subsection (2) outlines that the Secretary of State is permitted to revise and reissue the code from time to time. Subsection (3) specifies that, before preparing or revising the code, the Secretary of State is required to consult with such persons as deemed appropriate. Subsection (4) stipulates that the code may contain different provisions for different purposes, including variations for different categories of regulated persons as well as transitional or saving provisions. 208. Subsection (5) clarifies that "regulated person" is the same as in Chapter 3.

Clauses 38 - 41

40. Clause 38 clarifies how the code of practice will be used and treated in legal and regulatory settings.

41. Clause 39 allows the Secretary of State to withdraw the code of practice and sets out the process for doing so.

42. Clause 40 sets out requirements for the Secretary of State to report on the operation of network and information systems legislation. The Secretary of State may require regulators to provide information in connection with these reporting requirements.

43. Clause 41 gives further detail on what regulations made under clause 24 and Chapter 3 of Part 3 may contain.

Clauses 45 - 52

44. Clause 45 gives the Secretary of State the power to delegate the monitoring of compliance with a direction to a regulator. Regulators may be directed to request information relating to compliance and report this information to the Secretary of State. This section also makes provision for the Secretary of State to disclose these reports.

45. Clause 46 gives the Secretary of State and regulators the power to issue an information notice to require a person to provide information which is reasonably required to exercise the functions granted in Part 4 of the Bill.

46. Clause 47 gives the Secretary of State and regulators the power to carry out inspections to assess compliance with a direction or a confirmation decision. The Secretary of State and regulators are also able to appoint a person to carry out an inspection on their behalf.

47. Clause 48 gives the Secretary of State and the regulators the power to issue a notification of contravention where there are reasonable grounds to suspect a person has not complied with requirements as set out in Part 4 of the Bill.

48. Clause 49 outlines the penalties that can be imposed for non-compliance and grants the Secretary of State the power to make regulations to define the calculation of turnover for penalties.

49. Clause 50 gives enforcement authorities the power to issue confirmation decisions where a person has been given a notification of contravention under clause 48, and where the enforcement authority is satisfied that non-compliance has taken place. The confirmation notice sets out the final decision and can require a penalty to be paid.

50. Clause 51 sets out how penalties may be enforced in England and Wales, Scotland and Northern Ireland. This clause gives regulatory authorities powers to

enforce penalties issued under clause 50, which is a modification to their functions.

51. Clause 52 sets out how breaches of non-disclosure requirements will be enforced, including the process for enforcement and the associated penalties.

Clause 56

52. Clause 56 sets out the conditions in which the Secretary of State or a regulator may disclose information for national security purposes. Whilst national security is reserved, the discretion to share information for that purpose under the Bill is a new function for regulatory authorities.

The Welsh Government's position

53. The LCM sets out the Welsh Government's reasons for making provision for Wales in the Bill. It says:

> *"Welsh Government supports extending regulators' powers over critical suppliers, addressing a gap in the current NIS Regulations. Following the 2022 Advanced ransomware attack on Welsh patient data, Welsh Government's 'Once for Wales' and 'defend as one' approach recognises suppliers as a major risk. New guidance via secondary legislation will enable a risk-based, cross-border response. Similarly, and in relation to the drinking water sector, the Welsh Government supports the Bill's objective of strengthening cyber defences. The Independent Water Commission's final report highlighted gaps in the industry's security arrangements and referred to an increasing number of cyber incidents. A cross-border approach is considered an effective means of safeguarding infrastructure and maintaining cyber resilience across the drinking water sector."*[6]

54. In the LCM, the Counsel General and Minister for Delivery also sets out her reasons for making these provisions in a UK Bill rather than utilising a Senedd Bill:

> *"The provision made in the Bill relates to the reserved matters of telecommunications and wireless telegraphy (Schedule 7A, C 9; para 83) and national security (B 3 para 32).*

[6] Welsh Government, Legislative Consent Memorandum on the Cyber Security and Resilience (Network and Information Systems) Bill paragraph 124

However, an LCM is nonetheless required as a number of provisions in the Bill confer, remove or modify functions of the Welsh Ministers and/or 15 Devolved Welsh Authorities (DWAs) or otherwise have regard to devolved matters as detailed above."[7]

55. The Welsh Government recommends that the Senedd gives its consent to the LCM. In the LCM, the Counsel General and Minister for Delivery states:

"I support this Bill and would recommend the Senedd consents to its provision. However, given the anticipated UK Parliamentary timetable of the Bill it is likely that a legislative consent debate on this Bill would - based on our established approach on seeking to schedule such debates after the Committee Stage in the Second House - take place in the next Senedd Term."[8]

Financial implications

56. In relation to the financial implications of the Bill, the LCM states:

"The legislative changes are expected to increase costs for water companies to meet enhanced cyber resilience requirements, potentially affecting future price reviews. There are also likely to be implications for the Drinking Water Inspectorate due to greater regulatory responsibilities. In the health sector, expanding the scope to include critical suppliers— many of whom are not currently covered by NIS Regulations—raises financial considerations. The fragmented nature of supplier arrangements across Wales means a significant pre-implementation scoping exercise will be needed to accurately assess costs and identify technical solutions for centralisation."[9]

[7] Welsh Government, Legislative Consent Memorandum on the Cyber Security and Resilience (Network and Information Systems) Bill paragraphs 125-126
[8] Welsh Government, Legislative Consent Memorandum on the Cyber Security and Resilience (Network and Information Systems) Bill paragraph 128
[9] Welsh Government, Legislative Consent Memorandum on the Cyber Security and Resilience (Network and Information Systems) Bill paragraph 127

3. Our view

57. We considered the LCM during a Committee meeting on 21 January 2026.

58. We note that the provisions of the Bill relate to reserved matters such as telecommunications and wireless telegraphy and national security. However, the Bill makes provision which confers, removes or modifies functions of the Welsh Ministers and/or devolved Welsh authorities, and therefore requires consent. The Bill also includes provision which increases, or could increase in the future, the regulatory burden on water companies, whose area is wholly or mainly in Wales, that supply drinking water. The regulation of this is devolved.

59. We note that the increased regulatory burden on water companies could lead to increased costs, as they will be required to meet enhanced cyber resilience requirements. We are concerned about the potential impact of this on customer bills, which have already increased substantially following the last price review. We would therefore be grateful for clarification on whether any assessment has been made of the additional cost to water companies in Wales.

60. We appreciate that the Bill, by addressing the gap in the current NIS Regulations, will ensure that we are not at increased risk of cyber attacks. Strengthening cyber resilience and providing greater protections for service users is important. We therefore see no reason why Senedd should not grant its consent in relation to the relevant provisions of the Bill.