

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

October 2026

1. Background

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 2025.¹ The Bill was re-introduced at Report Stage on 14 May 2026 following the King's Speech.

2. The Bill is sponsored by the Department for Science, Innovation and Technology.

3. 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.”

4. 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

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



Regulations”), as well as delivering new powers with the aim of ensuring government can respond to new and emerging cyber threats.

5. 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. 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. The Bill’s Explanatory Notes state that 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.”²

7. Twelve regulators oversee the enforcement of the NIS 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 Ministers in their role as regulator, including with new powers to designate critical supplies, and 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.

² HL Bill 32-EN, **Cyber Security and Resilience (Network and Information Systems) Bill, Explanatory Notes** (to the Bill as introduced to the House of Lords on 17 June 2026)

Legislative Consent Memorandum in the Sixth Senedd

10. Standing Order 29.1 provides that the Welsh Ministers must lay a Legislative Consent Memorandum where a UK Bill makes provision in relation to Wales that has regard to devolved matters.³

11. Julie James MS, the then Counsel General and Minister for Delivery, laid a Legislative Consent Memorandum on the Bill on 25 November 2025, which was considered by Members of the Sixth Senedd.⁴

12. The then Climate Change, Environment and Infrastructure Committee laid its report on 9 February 2026.⁵ The Welsh Government responded to the report on 20 March 2026.⁶

13. The then Legislation, Justice and Constitution Committee laid its report on 12 February 2026.⁷ The Welsh Government responded to the report on 20 March 2026.⁸

14. A legislative consent motion was not tabled prior to the dissolution of the Senedd on 8 April 2026 and so no vote took place in the Sixth Senedd.

Legislative Consent Memorandum in the Seventh Senedd

15. Adam Price MS, Cabinet Minister for Enterprise, Connectivity and Energy (“the Cabinet Minister”), laid a Legislative Consent Memorandum (“the LCM”) on 9 June 2026.⁹

³ **Standing Orders of the Welsh Parliament**, April 2026

⁴ Welsh Parliament, **Legislative Consent: Cyber Security and Resilience (Network and Information Systems) Bill (2024-26)**

⁵ 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

⁶ Welsh Government, **Cyber Security and Resilience (Network and Information Systems) Bill: Response to the Climate Change, Environment and Infrastructure Committee Report on the Legislative Consent Memorandum**, March 2026

⁷ Legislation, Justice and Constitution Committee, **The Welsh Government’s Legislative Consent Memorandum on the Cyber Security and Resilience (Network and Information Systems) Bill**, February 2026

⁸ Welsh Government, **The Welsh Government’s Legislative Consent Memorandum on the Cyber Security and Resilience (Network and Information Systems) Bill: Welsh Government response to the Legislation, Justice and Constitution Committee’s report**, March 2026

⁹ Welsh Government, **Legislative Consent Memorandum: Cyber Security and Resilience (Network and Information Systems) Bill**, June 2026

16. On 16 June, the Business Committee referred the LCM to the Economy, Energy and Connectivity Committee (“the Committee”), and the Legislation Committee, with a reporting deadline of 9 October 2026.¹⁰

2. The LCM

Provisions requiring consent

17. Paragraphs 14 – 122 of the LCM set out the Welsh Government’s view as to which provisions in the Bill require the consent of the Senedd. Paragraphs 123 and 124 clarify the difference in position regarding consent between the UK and Welsh Governments:

“DSIT have provided a Devolution Analysis which states that consent is required for Clauses 12, 17, 19, 20, 22, 29, 31, 32, 33, 45, 48, 49, 50 and 51.

I agree with this assessment but, for the reasons outlined above, assess that consent is also required for clauses 15, 18, 21, 25, 27, 28, 30, 34, 35, 36, 38, 39, 40, 41, 46, 47, 52 and 56.”¹¹

18. The clauses requiring consent are detailed below.

Part 2 – clauses 12 to 22

19. 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

¹⁰ Business Committee, **Timetable for consideration: Legislative Consent Memorandum on the Cyber Security and Resilience (Network and Information Systems) Bill**, June 2026

¹¹ There is a discrepancy between English and Welsh language versions of the LCM relating to the clauses listed in paragraphs 123 and 124. However Annex A to the **Explanatory Notes to the Bill** as introduced to the House of Lords on 17 June 2026 makes clear the provisions for which the UK Government considers consent of the Senedd is required, namely 12, 17, 19-22, 27-29, 31-35, 45-51 and 56. This is further confirmed in a letter from the Cabinet Minister to the Legislation Committee on **1 September 2026**.

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

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

21. Clause 17 amends the NIS Regulations related to the ability of regulators to impose charges to cover the full cost of their regulatory duties.

22. 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.

23. 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.

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

25. 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.

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

Part 3 – clauses 25 to 41

27. Clause 25 makes provision about the designation of 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 provides 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.

28. Subsections (3) to (8) of clause 25 make provision for the statement, including requirement for publication, and provisions for amending and withdrawal of the statement.

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

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

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

32. 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 out 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) define 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. Subsections (5) and (6) clarify what is meant by the terms “security or operational compromise,” and “service-critical supply” within the Chapter.

33. Clause 30 relates to the imposition of requirements on regulated persons. 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, including the definition of “regulated persons” for the purposes of Chapter 3, and a non-exhaustive list of specific requirements that may be imposed on regulated persons.

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). Subsections (2) to (6) add more detail and clarity about those regulations, including about what may be included about the disclosure of information, 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, and 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.

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. 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. Subsections (2) to (5) make further provision around the code, including that, before preparing or revising the code, the Secretary of State is required to consult with such persons as deemed appropriate.

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.

Part 4 – clauses 45 to 56

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.

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

Reasons for making provisions for Wales in the Bill

53. Paragraphs 125 to 128 set out the reasons for making those provisions for Wales in the Bill. It is stated that the Welsh Government “supports extending regulators’ powers over critical suppliers, addressing a gap in the current NIS Regulations”, and further, that “New guidance via secondary legislation will enable a risk-based, cross-border response.”

54. Paragraph 126 adds:

“A cross-border approach is considered an effective means of safeguarding infrastructure and maintaining cyber resilience across the drinking water sector.”

Financial implications

55. Paragraph 129 states that:

“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.”

56. It states that, while the Department for Science, Information and Technology published an Impact Assessment alongside the Bill, which considers the expected impacts on regulated entities and which would include the water sector, “at this stage, the analysis is not disaggregated into a water sector level, water company level or a Wales specific level.”

57. Paragraph 130 also notes:

“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.”

Welsh Government position on consent

58. The LCM does not indicate whether the Welsh Government recommends that the Senedd gives its consent to the Bill. Instead it notes that the Cabinet Minister “will continue to monitor and provide updates on this Bill's passage through Parliament”, and that a recommendation on consent will be brought forward “once Welsh Government has analysed the wider impact of the UK legislative programme for Wales.”¹²

3. Committee consideration

59. The Committee considered the LCM at its meeting on 8 July 2026,¹³ and subsequently wrote to the Cabinet Minister seeking further clarity in relation to the potential cost implications for Wales and the Welsh Government's position on consent.¹⁴

60. In response, the Cabinet Secretary said:

¹² Welsh Government, **Legislative Consent Memorandum: Cyber Security and Resilience (Network and Information Systems) Bill**, June 2026, paragraph 131

¹³ **Economy, Energy and Connectivity Committee, 8 July 2026**

¹⁴ **Letter to the Cabinet Minister for Enterprise, Connectivity and Energy**, 14 July 2026

“the NHS Wales Cyber Resilience Unit has been working with Health Operators of Essential Services (OES) as part of pre-implementation activity. This on-going work includes briefings on the future regulation of designated critical suppliers, highlighting senior level ownership and advising the OES of initial preparation measures such as review and assessment of current cyber risk mitigation measures taken in relation to existing suppliers; these briefings and review are ongoing. In parallel, Digital Health and Care Wales are testing a potential technological solution to identify and collate relevant critical suppliers centrally, which could be deployed across the NHS estate. As this work is at an early stage, potential costs have not yet been identified.”¹⁵

61. With regard to the potential impact on water companies, the Cabinet Secretary said that “Defra has confirmed that there are no current plans for the UK Government to undertake an analysis of water sector specific costings associated with the Bill”, but added that:

“Welsh Government will continue to engage with the UK Government during implementation of the Bill and the development of any secondary legislation the Bill makes provision for. During this time, we will also work with water companies themselves to assess cost implications.”

62. The Cabinet Secretary also confirmed that, to date, the Welsh Government had not sought any amendments to the Bill. He noted that while he is supportive of the Bill’s objectives, he will “formally update the Senedd regarding the legislative consent position shortly”.

63. On 28 September 2026 the Cabinet Minister wrote a further letter to the Committee to confirm that:

“As a result of ongoing engagement with UK Government, I can confirm that the Welsh Government can now recommend the Senedd give their consent for the relevant provisions of the Bill.”¹⁶

¹⁵ **Letter from the Cabinet Minister for Enterprise, Connectivity and Energy**, 1 September 2026

¹⁶ **Letter from the Cabinet Minister for Enterprise, Connectivity and Energy**, 28 September 2026

Committee view

64. The Committee notes the Welsh Government's view as to which provisions within the Bill require the consent of the Senedd, and we agree that consent is needed for those provisions. However, we note that clause 37(7) enables the Secretary of State to amend clause 36 (so far as it relates to consultation) by regulations.

65. This would enable the Secretary of State to amend section 36(3), which includes a requirement for the Secretary of State to consult such persons as the Secretary of State deems appropriate. This could affect what the final code of practice would contain, depending on who was consulted. The Secretary of State therefore has both discretion as to who is consulted, and the ability to change the fundamental consultation requirement. The Welsh Government states that clause 36 requires consent, but its rationale for not including clause 37(7) of the Bill in its list of provisions requiring consent is unclear.

Recommendation 1. The Cabinet Minister should explain the Welsh Government's position on whether consent is required for clause 37(7) of the Bill.

66. We note the Welsh Government's view that a cross-border approach is considered an effective means of safeguarding infrastructure and maintaining cyber resilience.

67. However we also note that, while the Welsh Government recognises there are likely to be increased costs, there is little information available on the implications of these potential costs to Wales and Welsh customers. We acknowledge the Cabinet Minister's comments that work is on-going in this regard and it is essential that it is continued, at pace, to ensure that any potential impacts are fully understood prior to the Bill's implementation.

Conclusion 1. The Cabinet Minister should keep this Committee informed as work progresses on assessing potential impacts of the Bill's implementation.

68. Finally, we note that the Cabinet Secretary has confirmed that the Welsh Government recommends that the Senedd gives its consent to the relevant provisions of the Bill, yet no further detail has been provided on the discussions with the UK Government which have led to this position.

Recommendation 2. The Cabinet Minister should provide further detail on the discussions held with the UK Government which have led to the Welsh

Government's decision to recommend consent, in advance of the Plenary debate on the Legislative Consent Motion.

69. As set out above, a number of issues relating to the LCM remain unclear. Therefore as a Committee we have been unable to reach a position on whether the Senedd should agree the Legislative Consent Motion associated with the LCM.

Conclusion 2. The Committee has not been able to reach a position on whether the Senedd should agree the Legislative Consent Motion associated with the LCM.