EFW/S6/26/7/1

Economy and Fair Work Committee
Wednesday 4 March 2026
7th Meeting, 2026 (Session 6)

Legislative consent memorandum on the Cyber Security and Resilience (Network and Information Systems) Bill (UK Parliament legislation)

Note by the Clerk

1. Legislative consent memorandum LCM-S6-70 was lodged on 6 January 2026 by Angela Constance MSP, Cabinet Secretary for Justice and Home Affairs and has been referred to the Economy and Fair Work Committee for scrutiny.

2. The LCM is available on the Scottish Parliament website and is included at **Annexe A**.

Cyber Security and Resilience (Network and Information Systems) Bill

3. The Cyber Security and Resilience (Network and Information Systems) Bill was introduced by Liz Kendall MP, Secretary of State for Science, Innovation and Technology in the House of Commons on 12 November 2025.

4. The Bill and associated documents can be viewed on the UK Parliament website.

5. The purpose of the Bill is to strengthen the UK's defences against cyber-attacks and improve the security and resilience of critical infrastructure, including by—

   - amending the Network and Information Systems Regulations 2018 and giving enhanced powers to competent authorities, including in relation to information sharing, incident reporting and enforcement;

   - giving the Secretary of State powers to further specify which activities should be regulated and by which authority; make regulations relating to the security and resilience of network and information systems; designate a statement of strategic priorities; and issue a code of practice for regulatory authorities; and

   - giving the Secretary of State the power to direct regulators and regulated bodies where threats relating to network and information systems pose a risk to national security.

6. The Bill had its Second Reading in the House of Commons on 6 January and has now completed its Committee stage. A carry-over motion has been lodged in the House of Commons to allow the Bill to continue its progress in the next parliamentary year (following the summer).

Legislative consent procedure

7. Under the Sewel Convention, the UK Parliament does not normally legislate on devolved matters or alter the legislative competence of the Parliament or the executive competence of the Scottish Government, without the consent of the Scottish Parliament. Consent is given by means of a resolution of the Parliament.

8. Under Chapter 9B of the Standing Orders, the Scottish Government must lodge a legislative consent memorandum (LCM) in relation to each UK Parliament Bill that contains provision ("relevant provision") that would require the Parliament's consent under the Convention. Sometimes the Scottish Government may be required to lodge one or more supplementary LCMs during the passage of a Bill. It is also possible for an LCM to be lodged by an individual MSP.

9. Every LCM lodged is referred to a lead committee for scrutiny and may also be referred to other committees. If the Bill confers power on the Scottish Ministers to make subordinate legislation, the Delegated Powers and Law Reform Committee (DPLRC) must also consider the LCM and may report on it to the lead committee.

10. Once the lead committee has reported, the Scottish Government normally lodges a motion on legislative consent for consideration in the Chamber. Such a motion may give consent to relevant provision in the Bill, refuse consent to such provision, or a mixture of the two. A draft of the motion is normally included in the LCM.

The Scottish Government's LCM

11. The Scottish Government and UK Government are not currently in agreement on which aspects of the Bill require consent (paragraphs 10 – 15 of the LCM).

12. The Scottish Government is recommending that legislative consent is given for clauses 12, 15, 17-23, 33, 38, 40, 46-52, 56 and Schedules 1 and 2. Detailed reasons for this are given in the LCM at paragraphs 18 to 58. Broadly, this is because they expand and/or improve the existing cyber security regime.

13. However, the Scottish Government has also identified clauses where it does not currently recommend that legislative consent is given. It has made no recommendation in relation to these. These are clauses 25, 26, 27, 28, 29, 30, 31, 32, 34, 35, 41, and 45. It notes (paragraph 59 of the LCM)—

> "These provisions concern the conferral of regulation making powers on the Secretary of State, which could be exercised in relation to devolved matters but do not require the consent of the Scottish Ministers."

14. The Scottish Government is in discussion with the UK Government on these clauses. As a carry-over motion has been lodged, this is likely to continue into

Session 7. Upon conclusion, the Scottish Government expects to lodge a further LCM setting out its final position.

15. The draft motion on legislative consent is as follows—

> That the Parliament agrees that the relevant provisions of the Cyber Security and Resilience (Network and Information Systems) Bill, introduced in the House of Commons on 12 November 2025, relating to clauses 12, 15, 17-23, 33, 38, 40, 46-52, 56 and Schedules 1 and 2, so far as these matters alter the executive competence of the Scottish Ministers, should be considered by the UK Parliament.

Evidence received

16. The Association of British Insurers submitted written views on the provisions of the Bill, included at **Annexe B**.

Evidence session

17. The Committee will hear evidence on the Scottish Government LCM from—

- Angela Constance, Cabinet Secretary for Justice and Home Affairs;
- Paul Chapman, Head of Public Sector Cyber Resilience, Scottish Government.

Next steps

18. Following this evidence session, members are invited to—

- **decide what recommendation to make to the Parliament – in particular, whether to recommend agreement to the Scottish Government's draft motion; and**

19. agree to consider a draft report in private at its next meeting.

Clerk to the Committee
February 2026

Legislative Consent Memorandum

Cyber Security and Resilience (Network and Information Systems) Bill

Background

1. This Memorandum has been lodged by Angela Constance MSP, Cabinet Secretary for Justice and Home Affairs, under Rule 9B.3.1(a) of the Parliament's Standing Orders.

2. The Cyber Security and Resilience (Network and Information Systems) Bill ("the Bill") was introduced by the UK Government in the House of Commons on 12 November 2025. The Bill, Explanatory Notes and other supporting documents can be found on the UK Parliament website at: Cyber Security and Resilience (Network and Information Systems) Bill - Parliamentary Bills | UK Parliament.

3. The Bill makes provision about the security and resilience of network and information systems which are used by or relied on for critical services in the UK. Its intention is to strengthen the UK's defences against the growing threat of cyber attacks and the associated disruption to critical services which could occur as a result.

4. At the moment, the main legislative scheme in this area is contained in the Network and Information Systems Regulations 2018 ("the NIS Regulations"), which set out a regulatory regime for the "essential services" of transport, energy, drinking water, health and digital infrastructure. It seeks to ensure that persons providing those services have adequate cyber security measures in place. The NIS regulations were made by the Secretary of State, prior to the United Kingdom's exit from the European Union as a result of an EU Directive on Security of Network and Information Systems Security 2016/1148 (known as the NIS Directive) which was adopted by the European Parliament on 6 July 2016.

5. The NIS Regulations designate "competent authorities" who are responsible for regulating specific sectors. In Scotland, the Scottish Ministers are designated as the competent authority for the health sector and the Drinking Water Quality Regulator for Scotland is designed as the competent authority for the drinking water supply and distribution sector.

Content of the Cyber Security and Resilience (Network and Information Systems) Bill

6. The Bill makes provision, including provision amending the NIS Regulations, about the security and resilience of network and information systems used or relied on in connection with the carrying on of essential activities.

7. The NIS Regulations apply to energy, transport, water and healthcare, online marketplaces, search engines and Cloud computing services. The regulations require:

- designated competent authorities to regulate specific sectors. As noted above, the Scottish Ministers are the designated competent authority in Scotland for the health sector and the Drinking Water Quality Regulator is the designated competent authority for the drinking water sector;
- relevant operators to take appropriate security measures and report incidents that significantly impact the continuity of their services.

8. The Bill is in five parts. For the purposes of this memorandum, the following parts are of particular relevance:

- Part 2 of the Bill amends the NIS Regulations to protect more digital services and supply chains, such as data centres, large load controllers, managed service providers and designated critical suppliers. It also gives enhanced powers to competent authorities, including in relation to information sharing, incident reporting and enforcement;
- Part 3 of the Bill confers powers on the Secretary of State to further specify activities which are to be regulated and to designate regulatory authorities to carry out that regulation. It also gives the Secretary of State powers to designate a statement of strategic priorities, to issue a code of practice for regulatory authorities and a power to make regulations “relating to the security and resilience of network and information systems which are used or relied on in connection with the carrying on of essential activities;
- Part 5 of the Bill gives the Secretary of State the power to give directions to regulated persons and regulatory authorities, where threats relating to network and information systems pose a risk to national security.

9. Network and information systems support a wide range of functions in the health and drinking water sectors in Scotland and therefore the Bill will have direct implications for these.

Provisions which require the consent of the Scottish Parliament

10. The Bill is a relevant Bill under Rule 9B.1.1 of the Standing Orders.

11. The Bill's provisions relate to matters which are reserved under schedule 5 of the Scotland Act 1998: national security (Head B8) and wireless telegraphy (Head C10). It is not within the legislative competence of the Scottish Parliament to make provision for the purpose of those reserved matters.

12. The Bill also alters the executive competence of the Scottish Ministers in their role as a designated competent authority under the NIS Regulations. This includes new powers, the expansion of existing powers and also new legal duties with which the Scottish Ministers would have to comply.

13. The Scottish Government considers that legislative consent is required in relation to clauses 12, 15, 17-23, 25-35, 38, 40, 41, 45-52, 56, schedule 1 and schedule 2.

14. The UK Government view is that consent is required for clauses 12, 17, 19-22, 27-29, 31-35, 45-51 and 56.

15. As such, the Scottish Government is of the opinion that consent is also required for clauses 15, 18, 23, 25, 26, 30, 38, 40, 41, 52 and schedule 1 and 2.

16. A full discussion of each clause, and the associated requirement for legislative consent, is attached at **Appendix A**.

Reasons for recommending legislative consent

17. The Scottish Government supports the Bill's overall aims as they are designed to enhance the regulation, improve cyber security and resilience of key sectors. The Bill aligns with the visions and outcomes of the Scottish Government's Strategic Framework for a Cyber Resilient Scotland in terms of improving critical sectors' cyber security and resilience, including the devolved health and drinking water sectors.

18. The reasons for the Scottish Ministers recommending consent be given for clauses 2, 15, 17-23, 33, 38, 40, 46-52, 56 and schedules 1 and 2 are as follows:

19. **Clause 12** (critical suppliers). This allows competent authorities to designate persons as "critical suppliers" where certain conditions are met. As a competent authority under the NIS Regulations, this alters the executive competence of the Scottish Ministers because it would create a new power that could be exercised, along with procedural requirements to be followed. It also places a duty on

competent authorities to co-ordinate with certain other relevant regulators, when exercising their functions.

20. The Scottish Government recommends that legislative consent is given for clause 12 because it allows a wider range of persons to be regulated as “critical suppliers” under the NIS Regulations, which strengthens supply chain cyber security.

21. **Clause 15** (reporting of incidents by regulated persons). This amends the types of incidents that must be reported to competent authorities to include events capable of having an actual adverse impact on the operation or security of network and information systems, in addition to events which actually have such an effect. Competent authorities also have new powers to direct that regulated persons inform the public about any incidents. Whilst the Scottish Ministers’ incident reporting functions, as a competent authority, remain, in practice they operate differently.

22. The Scottish Government recommends that legislative consent is given for clause 15 because it broadens the range of incidents that require to be reported under the NIS Regulations and create stricter timescales, including a new requirement for initial notifications to be sent within 24 hours of an operator of essential services becoming aware that a cyber incident has occurred or is occurring.

23. **Clause 17** (powers to impose charges). This amends the power for competent authorities to impose charges under the NIS Regulations. It permits them to create charging schemes for the recovery of costs for the discharge of their functions under the NIS Regulations. As a competent authority, this is a new power for the Scottish Ministers.

24. The Scottish Government recommends that legislative consent is given for clause 17 because it expands the existing regime regarding the powers to impose charges.

25. **Clause 18** (sharing and use of information under the NIS Regulations). This broadens the range of persons with whom competent authorities can share information under the NIS Regulations. Although it does not create a legal obligation to share information, it does amount to a modification of existing rules and, as a competent authority, alters the Scottish Ministers’ executive competence.

26. The Scottish Government recommends that legislative consent is given for clause 18 as it permits the Scottish Ministers to share information more widely under the NIS Regulations.

27. **Clause 19** (guidance). This clause amends regulation 3 of the NIS Regulations to provide that guidance issued by competent authorities have to include certain things and that, whilst preparing that guidance, competent authorities must have to have regard to any relevant code which is in force and to co-ordinate and consult with other competent authorities. As a competent authority, this alters the

executive competence of the Scottish Ministers as it creates more prescriptive requirements than exist currently.

28. The Scottish Government recommends that legislative consent is given for clause 19 as it ensures that cyber security and resilience guidance issued by competent authorities covers specific key issues.

29. **Clause 20** (powers to require information). This replaces regulation 15 of the NIS Regulations with a new version of the power for competent authorities to require information from persons that are regulated by them. This includes a power to require such information or documents that a competent authority reasonably requires for the purpose of exercising or deciding whether to exercise any of its functions under these Regulations. As a competent authority, this amounts to an alteration of the Scottish Ministers' functions by expanding them.

30. The Scottish Government recommends that legislative consent is given for clause 20 as it creates expanded, clear powers for competent authorities to require information for the purpose of carrying out their functions.

31. **Clause 21** (financial penalties). Competent authorities do already have the power to impose financial penalties for non-compliance. This clause, however, creates a new power for competent authorities to serve a "notice of intention to impose a penalty" in certain circumstances. It also places a new legal duty on competent authorities to have regard to specific matters when determining whether a penalty is appropriate and proportionate in the circumstances. As a competent authority, this amounts to an alteration of the Scottish Ministers' executive competence.

32. The Scottish Government recommends that legislative consent is given for this clause as it strengthens the penalty regime and this also applies to any critical suppliers designated under clause 12.

33. **Clause 22 and schedule 1** (enforcement and appeals). This clause introduces schedule 1 of the Bill, which makes a number of changes to the enforcement powers which are available to competent authorities. This includes the powers available to the Scottish Ministers as a competent authority and thus alters their executive competence.

34. The Scottish Government recommends that legislative consent is given for clause 22 and schedule 1 as they strengthen enforcement action where duties are breached by regulated persons.

35. **Clause 23 and schedule 2** (minor and consequential amendments). This clause introduces schedule 2 of the Bill which makes minor and consequential changes which are needed in light of certain changes being made throughout the Bill. This includes removal of the existing regulation 21 of the NIS Regulations on fees and removal of the current requirement in regulation 3(6) for competent authorities to have regard to the NIS national strategy.

36. The Scottish Government recommends that legislative consent is given for clause 23 and schedule 2 as they support changes being made elsewhere in the Bill, which strengthen the regulation of cyber security such as the amendments to the current rules on fees.

37. **Clause 33** (regulatory authorities and other persons: information, guidance and other functions). This clause allows functions to be conferred on regulatory authorities in relation to certain things, when regulations are made under clause 29.

38. The Scottish Government recommends that legislative consent is given for clause 33 because it allows functions to be conferred on the Scottish Ministers and the Drinking Water Quality Regulator for Scotland, which could be for specific purposes including disclosure of information, giving of guidance, keeping of records, preparation of reports and carrying out reviews. Although this could increase the regulatory burden on regulatory authorities, this clause enables the sharing of information for the purposes of sharing best practice and lessons identified across sectors, including outside the UK.

39. **Clause 38** (effects of code of practice). This clause places a legal duty on regulatory authorities when determining whether a regulated person has complied with a requirement either (a) under regulations which were made under clause 29, or (b) a requirement in the NIS Regulations. The regulatory authority has to consider any provision of a code of practice which the Secretary of State may have issued under clause 36. This alters the functions of the Scottish Ministers as a competent authority and therefore amounts to an alteration of their executive competence.

40. The Scottish Government recommends that legislative consent is given for clause 38 because it ensures that regulatory authorities act appropriately, when determining any question relating to a regulated person's compliance.

41. **Clause 40** (report on network and information systems legislation). This clause places a requirement on the Secretary of State to lay before Parliament a report on the network and information systems legislation at least every 5 years. It places a legal obligation on regulatory authorities to provide such information as the Secretary of State thinks they "reasonably require" in order to publish that report. It therefore places a new legal obligation on the Scottish Ministers, as a regulatory authority and amounts to an alteration of their executive competence.

42. The Scottish Government recommends that legislative consent is given for clause 40 because it would require a report to be laid before parliament, setting out progress of regulatory authorities, the objectives intended to be achieved by the regulations and review the exercise of powers under the Bill. This allows for lessons to be learned and cyber security and resilience to be improved across the UK.

43. **Clause 46** (information gathering). This clause confers power on regulatory authorities to require regulated persons to provide information or documents they may reasonably require for the purpose of complying with a direction or request

issued under clause 45. As a regulatory authority, this is a new power for the Scottish Ministers and thus amounts to an alteration of their executive competence.

44. The Scottish Government recommends that legislative consent is given for clause 46 because it gives regulatory authorities enhanced powers to use in ensuring that regulated persons comply with the regulations for ensuring cyber security and resilience.

45. **Clause 47** (inspections). This clause would give regulatory authorities the power to carry out inspections in certain circumstances. As a regulatory authority, this amounts to an alteration of the Scottish Ministers' executive competence.

46. The Scottish Government recommends that legislative consent is given for clause 47 because it gives regulatory authorities the power to carry out inspections in certain circumstances, improving cyber security and resilience.

47. **Clause 48** (notification of contravention). This clause gives regulatory authorities the power to issue enforcement notifications where there are reasonable grounds to suspect that a person has not complied with requirements as set out in the Bill. As a regulatory authority, this amounts to a new power and thus an alteration of the Scottish Ministers' executive competence.

48. The Scottish Government recommends that legislative consent is given for clause 48 because it would give regulatory authorities the power to issue enforcement notifications in certain circumstances for the purposes of improving cyber security and resilience.

49. **Clause 49** (penalty amounts). This clause gives regulatory authorities the power to issue penalties for non-compliance and to determine the penalty amount in a contravention notice. As a regulatory authority, this amounts to a new power and thus an alteration of the Scottish Ministers' executive competence.

50. The Scottish Government recommends that legislative consent is given for clause 49 because it allows penalties to be issued in certain circumstances where standards in cyber security and resilience fall short of legal requirements.

51. **Clause 50** (enforcement of notification). This clause gives regulatory authorities the power to issue confirmation decisions in relation to enforcement notifications they issue under clause 49. A confirmation decision could require a penalty to be paid. As a regulatory authority, this amounts to a new power and thus an alteration of the Scottish Ministers' executive competence.

52. The Scottish Government recommends that legislative consent is given for clause 50 because it allows enforcement action to be taken where standards in cyber security and resilience fall short of legal requirements.

53. **Clause 51** (enforcement of penalty). This clause gives regulatory authorities the power to enforce penalties issued under clause 50. As a regulatory authority, this amounts to a new power and thus an alteration of the Scottish Ministers' executive competence.

54. The Scottish Government recommends that legislative consent is given for clause 50 because it allows enforcement action to be taken where standards in cyber security and resilience fall short of legal requirements.

55. **Clause 52** (enforcement of non-disclosure requirements). This clause gives regulatory authorities the power to enforce penalties for breach of non-disclosure requirements. It sets out the process for enforcement and the associated penalties.

56. The Scottish Government recommends that legislative consent is given for clause 52 because it gives regulatory authorities the power to enforce breaches of non-disclosure requirements. As a regulatory authority, this would amount to a new power and thus an alteration of the Scottish Ministers' executive competence.

57. **Clause 56** (information sharing). This clause gives regulatory authorities the power to share information with certain bodies, including to improve cyber security and resilience. As a regulatory authority, this amounts to a new power and thus an alteration of the Scottish Ministers' executive competence.

58. The Scottish Government recommends that legislative consent is given for clause 56 because it allows for increased information sharing, which could be used to enhance cyber security and resilience.

Provisions in relation to which the Scottish Government cannot currently make a recommendation on consent

59. The Scottish Government has also identified a number of clauses of the Bill which require the legislative consent of the Scottish Parliament but for which the Scottish Government does not currently recommend that consent is given. These provisions concern the conferral of regulation making powers on the Secretary of State, which could be exercised in relation to devolved matters but do not require the consent of the Scottish Ministers. These provisions are subject to ongoing discussion with the UK Government to understand why the UK Government thinks it is appropriate to take powers that could allow the Secretary of Statement to legislate in this way. The Scottish Government therefore is not presently in a position to recommend that the Scottish Parliament consent to these provisions. A Supplementary Legislative Consent Memorandum will be lodged when discussions with the UK Government have concluded.

60. The particular provisions, namely clauses 25-32, 34, 35, 41 and 45 are considered in turn below but, in general, the concern is to secure appropriate respect for devolved responsibilities in these provisions.

61. **Clause 25** (statement of strategic priorities etc). This clause allows the Secretary of State to designate a statement of strategic priorities. This will set out a number of things including the roles and responsibilities of regulatory authorities and the objectives for regulatory authorities, in seeking to give effect to those strategic priorities. This means that the Secretary of State could place new duties on regulatory authorities, including the Scottish Ministers, which amounts to an alteration of executive competence.

62. **Clause 26** (consultation and procedure in relation to statement). This clause places a requirement on the Secretary of State to consult with regulatory authorities on a draft of the strategic statement. This is a new legal entitlement for the Scottish Ministers, as a regulatory body, which amounts to an alteration of their executive competence.

63. **Clause 27** (duties of regulatory authorities in relation to statement). This places a legal obligation on regulatory authorities to have regard to the statement of strategic priorities, when exercising any of their functions and also to seek to achieve any relevant objectives set out in the statement. This alters the way in which regulatory authorities are required to carry out their functions. As a regulatory authority, this alters the executive competence of the Scottish Ministers.

64. **Clause 28** (report by Secretary of State). This requires the Secretary of State to lay before parliament, at the end of each reporting period, a report setting out, in general terms, how regulatory authorities have complied with their duties under clause 26 and are planning to comply with those duties in the subsequent reporting period. There is also a power, for the purpose of the report, for the Secretary of State to issue a notice to regulatory authorities, which requires the authority to provide such information as specified in the notice. As a regulatory authority, this applies to the Scottish Ministers and therefore alters their executive competence.

65. The Scottish Government is not presently in a position to make any recommendation to the Scottish Parliament as to whether consent should be granted for clauses 25 – 28. Regulatory authorities, including Scottish authorities, must have regard to the statement and seek to achieve any relevant objectives contained within it. The strategic statement will therefore influence the manner in which devolved statutory duties are exercised. Whilst clause 26 places a requirement on the Secretary of State to consult with regulatory authorities on a draft of the statement, there is no requirement to obtain the consent of the Scottish Ministers beyond the limitations of this consultation. The Scottish Government considers that this is required given that the statement alters the executive competence of the Scottish Ministers.

66. Clauses 29, 30, 31, 34 and 35. Clause 29 allows the Secretary of State to make further regulations relating to the security and resilience of network and information systems. This could include regulations in connection with the identification, management and reduction of risks in relation to relevant network and information systems and also the mitigation of adverse impacts. They could also confer functions on "regulated persons”, as a result of clause 30(1). This would include the Scottish Ministers, as a competent authority, as a result of the definition

in clause 24(8)(a). That clause states that persons designated as competent authorities under regulation 3(1) of the NIS Regulations are to be treated as being designed as a “regulatory authority” for the purposes of Part 3 of the Bill. Clause 29 amounts to an alteration of the executive competence of the Scottish Ministers.

67. Clauses 30, 31, 34 and 35 establish the parameters to shape the powers under clause 29 to make the new regulations.

68. The Scottish Government is not presently in a position to make any recommendation to the Scottish Parliament as to whether consent should be granted for clauses 29-31, 34 and 35. These provisions could be exercised in a way that confers functions on devolved regulatory authorities, including Scottish Ministers, without any requirement to consult or seek the consent of Scottish Ministers. These regulations are legally binding and could increase the regulatory burden on devolved operators of essential services.

69. **Clause 32** (provision about financial penalties). This clause permits the Secretary of State, when making regulations under clause 29(1), to make provisions for or in connection with the imposition of financial penalties by regulatory authorities. This may specify things including the amount of penalty to be imposed, how it is to be determined and how regulatory authorities are to deal with sums received. As a regulatory authority, this amounts to an alteration of the executive competence of the Scottish Ministers.

70. The Scottish Government is not presently in a position to make any recommendation to the Scottish Parliament as to consent for clause 32. A penalty imposed on a Scottish public authority would effectively be paid from the Scottish Consolidated Fund under section 64 of the Scotland Act 1998. The absence of any statutory requirement to consult the Scottish Ministers before effectively imposing financial liabilities on devolved bodies raises concerns about accountability to the Scottish Parliament for the use of public funds. A financial safeguard or consent mechanism is therefore required.

71. **Clause 41** (regulations under section 24 or Chapter 3). This clause gives the Secretary of State powers to make consequential amendments to primary legislation when making regulations under clause 24 or Chapter 3 of the Bill. Primary legislation is defined as including Acts of the Scottish Parliament. This clause confers a power on the Secretary of State to amend or repeal Acts of the Scottish Parliament through United Kingdom secondary legislation. Clause 41 therefore allows the Secretary of State to amend or repeal legislation that was made for a purpose within the legislative competence of the Scottish Parliament.

72. The Scottish Government is not presently in a position to make any recommendation to the Scottish Parliament as to consent for clause 41. In the Scottish Government’s view this is a significant constitutional issue. Section 28(8) of the Scotland Act 1998 recognises that the UK Parliament will not normally legislate on devolved matters without the consent of the Scottish Parliament. Clause 41 allows UK Ministers, rather than the UK Parliament, to modify devolved primary

legislation without any statutory requirement to obtain the consent of the Scottish Ministers. The Scottish Government therefore considers that clause 41 cannot be supported unless the Bill is amended to introduce a statutory consent mechanism or a joint regulation making power.

73. **Clause 45** (monitoring by regulatory authorities). This clause confers powers on the Secretary of State to direct regulatory authorities to do certain things. Although the Scottish Ministers are specifically excluded from that power, clause 45(9) gives them the authority to comply with a request made by the Secretary of State. Complying with such a request would amount to a new function for the Scottish Ministers as a regulatory authority and thus amounts to a modification of their executive competence. The direction-making power also covers the Drinking Water Quality Regulator for Scotland and amounts to a modification of its functions.

74. The Scottish Government is not presently in a position to make any recommendation to the Scottish Parliament as to consent for clause 45 as the Secretary of State is able to issue directions to devolved regulatory authorities which were not part of the Scottish Government, including the Drinking Water Quality Regulator for Scotland, and these directions could add additional burdens to devolved public bodies with no requirement to consult or seek consent of Scottish Ministers.

Consultation

75. The UK Government published a consultation on proposals for legislation to improve the UK's cyber resilience in January 2022. The UK Government's response was published in November 2022. The consultation and response established the clear need to expand the regulation of digital service providers and update the NIS Regulations to take account of lessons identified from the first 3 years of the implementation of the regulations.

Financial implications

76. There appears to only be minor cost potentially falling on the Scottish Government from the Bill, although the Bill allows for significant changes to be made to the scope of the NIS regulations in the future which could have a more significant impact. In addition, if Scottish Ministers were to exercise powers to designate critical suppliers to the health sector, many of whom are not currently covered by NIS regulations, this would raise financial considerations.

Post EU scrutiny

77. These provisions are relevant to the Scottish Government's policy to maintain alignment with the EU as they go some way to bridging the gap between the current NIS Regulations and the EU NIS2 Directive. In particular, the Bill aligns with NIS2 on incident notification timelines, regulation of managed service providers and encouraging alignment with established cyber security frameworks. The Bill also

creates the powers necessary to expand the scope of the NIS regulations and allow closer alignment in the future.

Conclusion

78. In conclusion, the Scottish Government agrees with the UK Government's view of the devolution position for this Bill in relation to the clauses they identified as requiring legislative consent (paragraph 14). However, the Scottish Government has highlighted further clauses which impact on devolved matters (paragraph 15).

79. The Scottish Government supports the overall aims of the Bill which should help to improve the cyber security and resilience of essential services in Scotland.

80. The Scottish Government is therefore recommending consent to clauses 12, 15, 17-23, 33, 38, 40, 46-52, 56 and Schedules 1 and 2 of the Bill.

81. The Scottish Government is still to reach a position on consent in relation to clauses 25-32, 34, 35, 41 and 45 as far as they relate to devolved matters.

Draft motion on legislative consent

82. The draft motion, which will be lodged by the Cabinet Secretary for Justice and Home Affairs, is:

> "That the Parliament agrees that the relevant provisions of the Cyber Security and Resilience (Network and Information Systems) Bill, introduced in the House of Commons on 12 November 2025, relating to clauses 12, 15, 17-23, 33, 38, 40, 46-52, 56 and Schedules 1 and 2, so far as these matters alter the executive competence of the Scottish Ministers, should be considered by the UK Parliament".

Scottish Government
January 2026

Appendix A

Cyber Security and Resilience (Network and Information Systems) Bill: Clauses which require legislative consent

1. **Clause 12 - Critical suppliers**. This clause enables a Designated Competent Authority (DCA) or the Information Commissioner to designate a person as a “critical supplier” within their sectors. These suppliers will then be subject to the NIS Regulations.

2. It places procedural requirements on DCAs in making a designation, including: (i) providing reasons to the person they are proposing to designate; (ii) taking into account any representation that person makes; and (iii) consultation requirements, including a requirement to consult certain other re levant regulators.

3. It also introduces a requirement for DCAs to co-ordinate with certain other relevant regulators in exercising their functions under the NIS Regulations.

4. As the Scottish Ministers are the DCA for health services in Scotland, this clause confers additional functions on them in that role.

5. **Clause 15 - Reporting of incidents by regulated persons**. New NIS regulation 11 requires regulated persons to make prescribed reports to the relevant DCA, which may be the Scottish Ministers.

6. The UK Government view is that this clause does not alter the functions of devolved governments or DCAs and that no LCM is therefore required.

7. However, this clause expands the type of incidents that are required to be reported under the NIS Regulations. Under new regulation 11B, the DCA is given functions in relation to notified incidents. The DCA is also given the power to direct the regulated person to inform the public about any incident.

8. This clause therefore alters the functions of the Scottish Ministers to the receipt of and response to incident reports under this provision. This provision also increases the regulatory burden on water companies that supply drinking water in Scotland, the regulation of which is devolved.

9. **Clause 17 - Powers to impose charges**. This clause amends the power for DCAs to impose charges under the NIS Regulations. 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 relate to the discharge of their regulatory duties under the NIS Regulations.

10. The Bill amends the existing cost recovery provisions which previously permitted DCAs to only recover costs directly.

11. This clause creates a new power to impose charges that regulators will need to consider exercising, as well as placing procedural requirements where they do wish to impose a charge – such as consulting on and publishing a charging scheme and producing a charging statement. This is therefore a modification to their functions.

12. **Clause 18 - Sharing and use of information under the NIS Regulations etc.**

13. The UK Government view is that this clause does not alter the functions of the Scottish Ministers or any devolved DCAs.

14. The UK Government considers that these provisions provide a gateway for information sharing, rather than putting a requirement for regulators (including the devolved governments) to share information.

15. They therefore do not consider this an alteration of functions.

16. Regulation 6 of the NIS Regulations already provides that the Scottish Ministers, as an NIS enforcement authority, may share information with each other for essentially the same purposes.

17. However, new regulation 6A (Other disclosures by a NIS enforcement authority) goes further, and provides that the Scottish Ministers, as an NIS enforcement authority, may disclose information to the Secretary of State if the authority considers that the information may be relevant for the purposes of a report under clause 40 of the Bill, or may otherwise assist the Secretary of State.

18. Clause 40(6) enables the Secretary of State to request information from regulators for the purposes of producing the report, which the regulators must then provide.

19. New regulation 6B (Onward disclosure of information received under regulation 6 or 6A) further extends the scope of this discretionary function.

20. This extended power to disclose for new purposes, together with the associated requirement to share information under clause 40(6), is an alteration of Scottish Ministers' functions.

21. **Clause 19 - Guidance**. This clause makes additional provision about what must be included in the guidance issued by DCAs under regulation 3 of the NIS Regulations.

22. This clause places requirements on regulators to issue guidance and specifies what it must include. This is more prescriptive than the existing requirement under the NIS Regulations and is therefore considered to be an additional function for regulators.

23. **Clause 20 - Powers to require information**. This clause gives DCAs additional powers to request information from any person that is regulated by them, or who they consider to be likely to have the information or documents sought, that they reasonably require in order to exercise, or decide whether to exercise, any of their regulatory functions under the NIS Regulations.

24. This extended power to require information for new purposes, together with the associated requirement to share information under clause 40(6), is considered to be a modification of Scottish Ministers' functions. This provision could also be exercised so as to increase the regulatory burden on water companies that supply drinking water in Scotland, the regulation of which is devolved.

25. **Clause 21 - Financial penalties**. This clause explains the circumstances in which DCAs may issue a regulated person with a penalty.

26. It also enables regulators to consider all relevant circumstances of a case when determining penalties, including patterns of non-compliance and proportionality of fine levels.

27. The clause also makes provisions relating to the penalty structure and introduces a new maximum penalty of 4% turnover, in addition to the current numerical cap of £17 million, whichever is higher.

28. The UK Government view is that this clause, as it relates to enabling DCAs to consider all relevant circumstances of a case when determining penalties, will modify the functions of regulators and that an LCM should be sought to that extent.

29. It is not considered that the provisions relating to penalty structures modify the functions of devolved governments - regulators can already impose penalties for non-compliance.

30. An LCM is therefore required for the provisions which enable regulators to consider all relevant circumstances of a case when determining penalties.

31. **Clause 22 - Enforcement and appeals**. Schedule 1 makes amendments to the NIS Regulations relating to enforcement and appeals. These provisions amend the enforcement powers available to regulators.

32. **Clause 23** - **Minor and consequential amendments etc.** Schedule 2 makes numerous amendments to the NIS Regulations including removal of regulations 21 (fees) and 3(6) (requirement for competent authorities to have regard to NIS national strategy).

33. The UK Government view is that clause 23 does not alter the functions of devolved governments.

34. However, whilst these are in consequence of changes being implemented elsewhere in the Bill, they would alter the functions of Scottish Ministers and devolved competent authorities in respect of fees and the national strategy authorities therefore trigger the need for the LCM.

35. **Clause 25 - Statement of strategic priorities etc**. This clause allows the Secretary of State to designate a statement of strategic priorities. The statement must set priorities, together with objectives for regulators relating to the priorities.

36. The UK Government view is that clause 25 does not alter the functions of devolved governments. It is the UK Government's position that whilst regulators will have to seek to achieve certain outcomes, how they do this will be for individual regulators to determine in the context of exercising their existing functions.

37. However, the statement of strategic priorities may make provision in relation to the roles and responsibilities of regulatory authorities to give effect to the stated priorities and set objectives for regulatory authorities in seeking to give effect to those priorities and in carrying out their roles and responsibilities. Therefore, in exercising this new power, the Secretary of may impose new duties on regulators.

38. Similarly, whilst the power to withdraw and amend a statement of strategic priorities lies with the Secretary of State, any withdrawn statement and/or amended statement may make provision in relation to the roles and responsibilities of regulatory authorities (including the Scottish Ministers) in giving effect to the stated priorities and set objectives for them. This could again affect a removal or a modification in the functions of the Scottish Ministers as regulator.

39. **Clause 26 - Consultation and procedure in relation to statement.** This clause places a requirement on the Secretary of State to consult with regulatory authorities on a draft of the strategic statement. This is a new legal entitlement for the Scottish Ministers, as a regulatory body, which would amount to an alteration of their executive competence.

40. **Clause 27 - Duties of regulatory authorities in relation to statement**. Clause 27 introduces requirements on regulators in relation to the designated statement of strategic priorities. Regulators must have regard to the statement whilst carrying out their regulatory functions and will have to exercise their functions in a way that seeks to achieve the outcomes in the statement.

41. Regulators will have to have regard to the strategic priorities set out by the Secretary of State when exercising their functions and seek to achieve any relevant objectives set out in the statement.

42. **Clause 28 - Report by Secretary of State**. The Secretary of State will be expected to issue a report on how the regulators sought to achieve the outcomes, for which the Secretary of State may request information from the regulators.

43. Subsections (4) and (5) set out that the Secretary of State may require a regulator to provide information for the purposes of compiling the report, through the issuing of an information notice.

44. This clause allows the Secretary of State to impose new duties on regulatory authorities for the purposes of the report, which must be complied with. A regulator in receipt of an information notice must provide the information by the deadline and in the format specified by the notice.

45. **Clause 29 - Regulations relating to security and resilience of network and information systems**. These clauses create a delegated power that enables the Secretary of State to make regulations for certain specified purposes relating to network and information systems.

46. This clause provides the Secretary of State with the power to make regulations for certain specified purposes. This may include regulations which confer functions on regulators.

47. The UK Government agrees that clause 29 provides the Secretary of State with the power to make regulations for certain specified purposes, including regulations which may confer functions on regulators. This provision could also be exercised to make regulations that increase the regulatory burden on water companies that supply drinking water in Scotland, the regulation of which is devolved.

48. **Clause 30 - Imposition of requirements on regulated persons**. 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.

49. Subsection (6) provides a non-exhaustive list of specific requirements that may be imposed on regulated persons, including requirements regarding the reporting of certain matters and disclosing information to regulators and other persons.

50. The UK Government view is that this clause does not alter the functions of devolved governments.

51. However, regulations made under this power could require regulated persons to provide information to regulators. The receipt of that information would be an additional function for regulators. This provision also supplements Clause 29 which, as previously noted, could be exercised to make regulations that increase the regulatory burden on water companies that supply drinking water in Scotland, the regulation of which is devolved.

52. **Clause 31 - Functions of regulatory authorities: enforcement, sanctions and appeals**. This clause allows regulations made under clause 29 to authorise regulators to take certain steps in relation to enforcement, sanctions and appeals.

53. The regulations made under this clause may impose additional functions on regulators.

54. The UK Government agrees that this clause allows regulations made under clause 29 to authorise regulators to take certain steps in relation to enforcement and financial penalties, which is a modification of their functions. This provision also supplements Clause 29 which, as previously noted, could be exercised to make regulations that increase the regulatory burden on water companies that supply drinking water in Scotland, the regulation of which is devolved.

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

56. Provision may include how regulatory authorities must deal with sums received by way of a penalty and recover unpaid penalties.

57. The UK Government agrees that this clause allows regulations to make provision in respect of financial penalties, so could be exercised to place functions on regulators in relation to financial penalties. This provision also supplements Clause 29 which, as previously noted, could be exercised to make regulations that increase the regulatory burden on water companies that supply drinking water in Scotland, the regulation of which is devolved.

58. However, it is the Scottish Government's position that a United Kingdom regulator or Minister should not create financial liabilities for devolved services without Scottish consent and penalties applied to Scottish public authorities must be paid from the Scottish Consolidated Fund and this engages section 64 of the Scotland Act. The Bill currently contains financial safeguards or joint framework provisions to support accountability to the Scottish Parliament.

59. **Clause 33 - Regulatory authorities and other persons: information, guidance and other functions**. This clause allows regulations made under clause 29 to confer additional functions on regulators relating to information sharing and guidance.

60. The UK Government agrees that this clause does confer new functions on regulatory authorities relating to information sharing and guidance. This provision also supplements Clause 29 which, as previously noted, could be exercised to make regulations that increase the regulatory burden on water companies that supply drinking water in Scotland, the regulation of which is devolved.

61. **Clause 34 - Recovery of costs of regulatory authorities**. This clause allows regulations made under clause 29 to make provision in respect of fees and therefore could be exercised to place functions on regulators in relation to fees.

62. The UK Government agrees that this clause allows regulations made under clause 29 to make provision in respect of fees, so could be exercised to place functions on regulators in relation to fees. This provision also supplements Clause 29 which, as previously noted, could be exercised to make regulations that increase the regulatory burden on water companies that supply drinking water in Scotland, the regulation of which is devolved.

63. **Clause 35 - Supplementary provision and interpretation**. Clause 35 adds supplementary detail on what regulations made under clause 29(1) may do, including the conferral of functions involving the exercise of a discretion; to provide for the delegation of functions by a regulatory authority; and to require a person to have regard to guidance or to a code of practice.

64. The UK Government agrees that this clause allows regulations to confer functions and provide for the delegation of functions by a regulatory authority. This provision also supplements Clause 29 which could be exercised to make regulations that increase the regulatory burden on water companies that supply drinking water whose area is wholly or mainly in Wales, the regulation of which is devolved.

65. **Clause 38 - Effects of code of practice**. Subsection (4) sets out that a regulator must take into account a provision of a code of practice issued under clause 36 when assessing compliance with requirements under clause 29(1) or the NIS Regulations if that provision of the code was active at the time the duties applied and appears to the regulator to be relevant.

66. The UK Government view is that this clause does not alter the functions of devolved governments, who will be overseeing compliance with the regulations. If issued, a code of practice would be used to help compliance with regulations which are reserved but would not change how the devolved governments or DCAs enforce the regulations.

67. However, sub-section (4) imposes a new duty on regulators to take account of any Code and thereby modifies the way in which they may exercise their functions.

68. **Clause 40 - Report on network and information systems legislation**. Clause 40 sets out requirements for the Secretary of State to report on the operation of network and information systems legislation.

69. Subsection (6) enables the Secretary of State to request information from regulators for the purposes of producing the report, which the regulators are required to provide.

70. The UK Government view is that this clause does not alter the functions of devolved governments.

71. However, the Secretary of State may require regulators to provide information in connection with these reporting requirements. This provision does therefore alter the functions of the Scottish Ministers in their role as a DCA.

72. **Clause 41 - Regulations under section 24 or Chapter 3**. The power for regulations to make consequential amendments includes power to amend or repeal provision made by primary legislation.

73. Primary legislation is defined as including an Act of the Scottish Parliament.

74. Consequential etc provision made to Scottish Parliament Acts under this power may therefore include relevant provision in relation to Scotland that has regard to devolved matters.

75. The UK Government view is that this clause does not require an LCM as it does not alter the functions of devolved governments or Devolved DCAs.

76. However, it is the Scottish Government's position that amending Acts of the Scottish Parliament in this way conflicts with Section 28(8) of the Scotland Act where it is recognised that the Parliament of the United Kingdom will not normally legislate with regard to devolved matters without the consent of the Scottish Parliament.

77. In addition, the functions of Scottish Ministers and other devolved DCAs could be altered by amendments to Acts of the Scottish Parliament

78. **Clause 45 - Monitoring by regulatory authorities**. This clause enables the Secretary of State to delegate the monitoring of compliance with a direction to a regulatory authority. Regulators may be directed to obtain information relating to compliance and report this information to the Secretary of State.

79. Whilst this clause provides that the Secretary of State may not issue a monitoring direction to the Scottish Government (defined in s. 44 of the Scotland Act as having Scottish Ministers as its members), the Scottish Government may be asked to comply with any equivalent request and exercise their powers to do so.

80. If the Scottish Ministers agree to comply with a request made by the Secretary of State under this provision, it would be a new function for them.

81. The UK Government agrees that this clause enables the Secretary of State to delegate the monitoring of the compliance with a direction to a regulator and that monitoring compliance with a national security direction is not a current function of the NIS regulators.

82. **Clause 46 - Information gathering.** Clause 46 gives 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 this Chapter of the Bill.

83. The UK Government view is that this clause does alter the functions of devolved governments or devolved DCAs. If exercised, the power would be used strictly for reasons of national security, which is a reserved matter.

84. However, subsection (2) grants the power for a relevant regulator to require a regulated person to provide information that the relevant regulator requires to comply with a monitoring direction or request issued under clause 45. If exercised, this would be a new function for them.

85. **Clause 47 - Inspections**. Where a regulatory authority is subject to a monitoring direction under clause 43 or a request has been made of it under clause 43(9), it may carry out all or any part of an inspection or appoint a person to do so.

86. The UK Government view is that this clause does alter the functions of devolved governments or DCAs. If exercised, the power would be used strictly for reasons of national security, which is a reserved matter.

87. However, clause 47 gives regulators the power to carry out inspections where they have accepted a request under section 45(9). This is a modification of their functions.

88. **Clause 48 - Notification of contravention**. Clause 48 gives 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 this Part of the Bill.

89. The UK Government agrees that this clause enables regulators to issue contravention notices, this includes financial penalties that the regulator is minded to impose, where a regulated entity has failed to comply with these requirements.

90. This provision gives regulators the power to issue a notification of contravention, which is a modification of their functions.

91. **Clause 49 - Penalty amounts**. Clause 49 outlines the penalties that can be imposed by enforcement authorities for non-compliance. It also grants the Secretary of State the power to make regulations to define the calculation of turnover for penalties.

92. Clause 49 gives regulators the power to determine the penalty amount in a contravention notice. This is a modification of their functions.

93. **Clause 50 - Enforcement of notification**. 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.

94. Clause 50 gives regulators the power to take enforcement action where a regulated entity has failed to comply with prescribed requirements. This is a modification of their functions.

95. **Clause 51 - Enforcement of penalty.** This clause provides that unpaid penalties are recoverable by enforcement authorities as a civil debt.

96. This clause gives regulatory authorities powers to enforce penalties issued under clause 50, which is a modification to their functions.

97. **Clause 52 - Enforcement of non-disclosure requirements**. Clause 52 sets out how breaches of non -disclosure requirements will be enforced, including the process for enforcement and the associated penalties. The UK Government view is that this clause does not alter the functions of devolved governments or devolved DCAs. If exercised, the power would be used strictly for reasons of national security, which is a reserved matter.

98. However, enforcement authorities may impose non-disclosure requirements under sections 48(9) and 50(9). An LCM is required for clauses 48 and 50. This provision relates to the enforcement of non-disclosure requirements imposed under those sections.

99. **Clause 56 - Information sharing**. This clause sets out the power of regulatory authorities to disclose information to other specified persons.

100. The UK Government agrees that this clause does alter the functions of devolved governments or devolved DCAs.

101. This provision gives power to regulatory authorities to share information where necessary for national security purposes.

102. Whilst national security is reserved, the discretion to share information for that purpose under the Bill is a new function for regulatory authorities.

This Legislative Consent Memorandum relates to the Cyber Security and Resilience (Network and Information Systems) Bill (UK Parliament legislation) and was lodged with the Scottish Parliament on 6 January 2026

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

© Parliamentary copyright. Scottish Parliamentary Corporate Body

Information on the Scottish Parliament's copyright policy can be found on the website - www.parliament.scot

Produced and published in Scotland by the Scottish Parliamentary Corporate Body.

All documents are available on the Scottish Parliament website at: www.parliament.scot/documents

Annexe B

Written submission from the Association of British Insurers

Executive summary

1. Cyber insurance is one the fastest growing product lines in the UK's world leading and innovative insurance industry, and our industry is well placed to address cyber risks and convene stakeholders to collectively improve the UK's cyber resilience.

2. Cyber risks, and especially ransomware, have been identified as top economic threats, as demonstrated by cyber-attacks on leading UK businesses, including M&S, Co-op, Harrods and Jaguar Land Rover.

3. We want to work with the government on our proposal to develop a strategic dialogue to clarify and align the expectations across businesses, insurers and the government to explore how best to work together to manage cyber risk and strengthen national cyber resilience.

4. We welcome the Cyber Security and Resilience Bill and the government's focus on strengthening the resilience of the UK's essential services and their supply chains against cyber-attacks through widening the scope of the Network and Information Systems (NIS) Regulations.

5. The Bill has the potential to benefit the entire economy by enhancing cybersecurity and improving resilience across a wide range of organisations. We believe that the industry has a role to play in supporting this goal.

6. While the Bill rightly addresses gaps in our Critical National Infrastructure's (CNI) cybersecurity, we also must address the cyber resilience of Small- and Medium-sized Enterprises (SMEs).

7. We support the government's proposal to introduce a mandatory cyber incident reporting regime for essential services and their supply chains to provide a clearer picture of the threat landscape.

8. We welcome, and strongly support, the government's ambitions to simplify and streamline regulation. It's important that the Bill's reporting requirements don't contradict the government's pledges to reduce regulation and duplication, especially as the financial services regulators develop their regime to regulate Critical Third Parties.

9. Clear guidance on what to report and when must be published in a timely manner to help regulated entities comply with the new regulations, as well as adopting a proportional approach, to ensure that requirements do not become overburdensome on SMEs.

Annexe B

Key asks for our sector

10. Continue to work with our sector to develop our proposal on a strategic dialogue to clarify and align the expectations across businesses, insurers and the government to explore how best to work together to manage cyber risk and strengthen national cyber resilience.

11. Clearly delineate the responsibilities of businesses, insurance, and government in cyber security and understand where the industry can and cannot support these goals.

12. Work with our sector to raise awareness of the value of cyber insurance and address the cyber resilience of SMEs.

13. Set out clear, objective definitions for who will be in scope of the Bill – specifically whether financial services institutions who operate their own data centres will be drawn into the scope of the NIS Regulations.

14. Clear and timely guidance for firms under the Bill's scope to help with compliance.

15. Ensure the reporting requirements set out in the Bill don't contradict the government's pledges to reduce regulation, duplication and costs for businesses and set out further detail on the exemption for small and micro-sized businesses.

16. Consider the appropriateness of the 24-hour and 72-hour timelines for reporting generally, and whether a tiered approach could be pursued for smaller regulated entities, which are less likely to have the capacity and in-house expertise to produce the reports on time.

Cyber insurance

17. Cyber insurance is a relatively new product, but it has matured in recent years, reflected by improved underwriting discipline, more clarity in policy wordings, and a better understanding of the overall risk landscape.

18. Cyber insurance is more than just an indemnity product that helps you to cover the costs of a malicious cyber incident or system outage. It offers proactive and reactive services to improve cybersecurity, detect issues early, prevent cyber-attacks from happening, and respond and recover if the worst happens. This service provision is a key driver of resilience.

19. Both the global and UK cyber insurance markets have grown at more than 20% per annum, with the UK market being forecasted to reach between £1.3 billion and £1.5 billion by 2027.

20. Last year, insurers paid out £197 million to help businesses recover from cyber incidents. Our data shows a 230% year-on-year increase in the amount

paid to support businesses with cyber-attacks, £138 million more than in 2023.

21. Recent incidents affecting M&S, Co-op, Harrods, and Jaguar Land Rover highlight the growing need to focus on the expectations and responsibilities of larger businesses. These firms are not only major employers and economic anchors, but also nodes in complex supply chains, meaning their resilience has far-reaching implications. The increasing reliance on critical vendors and suppliers, such as cloud infrastructure and software providers, is driving a concentration of risk across the wider economy.

22. Despite these recent major cyber-attacks, insurers are still keen to provide cover to more UK organisations, from SMEs to multinationals, and in 2025, we continued to see excess capacity in the market.

23. We're working with the London Market Association and BIBA to create a template cyber insurance wording and underwriting glossary of commonly used cyber terminology in partnership with insurers and regulators to help increase understanding of what cyber insurance can offer.

24. We've proposed the government establishes a strategic forum to clarify and align expectations across large businesses, insurers and government to explore how best to work together to manage cyber risk and establish a framework to strengthen national cyber resilience.

SMEs

25. While the Bill rightly focuses on building the resilience of our critical national infrastructure, more must be done to address the cyber resilience of Small and Medium-sized Enterprises (SMEs).

26. The take up of cyber insurance by UK SMEs is very low. Different methods are used to calculate insurance penetration, but reliable estimates can vary and range from 10%-40%. Last year, we published our Cyber Resilience for SMEs: The Insurance Gap Explored report, exploring how cyber insurance can help to prevent and alleviate the impact of cyber-attacks for SMEs. As recommended in our report, we want to work with the government to raise awareness of the value cyber insurance offers, both in helping to improve businesses' cyber defences and to help them withstand and survive a cyber-attack.

27. Our Cyber Safety Tool, a free, interactive tool also helps SMEs assess their own cyber security and plug any identified gaps in their cyber resilience. Our Cyber Safety Tool has been created using expertise from within the insurance industry and utilises identified best practice and protocols from the National Cyber Security Centre (NCSC).

28. As cyber risks continue to grow, SMEs are typically more vulnerable and less well placed than larger businesses to respond to cyber threats, generally due to overstretched resources, including IT and potential security gaps.

29. Only 25% of medium-sized businesses, according to research by Public First and the ABI, hold cyber insurance cover. 57% of respondents to the survey have software or cloud services, but only 29% have cyber insurance protection. For SMEs with a physical premises, of those who have software or cloud services, 32% have cyber insurance protection.

30. Our report, commissioned by the ABI with Public First, Small Business, Big Risk: Tackling SME Underinsurance, explores the uninsurance and underinsurance of SMEs setting out the industry's commitment to increasing SME's resilience alongside a guide for SMEs explaining insurance products, how to find the right products for their business, and the value of insurance.

Scope

31. The Bill significantly expands the scope of the Network and Information Systems (NIS) Regulations, resulting in more organisations having increased duties placed on them, including those likely to already have cyber insurance (such as cybersecurity and IT vendors), and potentially insurers. Provisions to designate organisations as critical suppliers also expand the scope of the regulations further.

32. The expansion of the regulations could mean cyber insurers or their supply chains come into the scope of regulation as operators of data centres or as providers of digital services such as continuous threat monitoring and other cybersecurity services. Insurers could potentially have a role to play in helping customers and designated critical suppliers to comply with the new duties, especially smaller organisations.

33. The Bill also updates existing duties for Relevant Digital Service Providers and makes equivalent provisions for Relevant Managed Service Provides and data centre operators to provide information to their regulators at the point of registration or designation. Insurers may want to help smaller providers by providing information on the new requirements to avoid potential fines for non-compliance.

34. The cost recovery framework for regulators to recover potential costs incurred in carrying out their new duties set out in the Bill will incur additional costs for businesses and organisations. Through imposing additional costs on businesses at a challenging time this measure could potentially deter organisations from taking out a cyber insurance policy in the first place, and lead to some opting not to renew their cyber insurance policy and spend less on other wider resilience measures.

35. If insurers are captured in the scope of the Bill, costs of compliance with the regulations would ultimately filter down to SME policyholders, who are already price sensitive.

36. We want to see clearer objective definitions for firms the Bill brings under its scope. While we appreciate this would likely become clearer as

the Bill undergoes further scrutiny, certainty is needed to help support businesses in future decision making and budget planning.

Reporting

37. We support the proposals within the Bill to introduce a mandatory cyber incident reporting regime for essential services and their supply chains. There's strong value in the government collating and publishing information about cyber incidents, potentially through an anonymised cyber incident database or exchange platform, which could help to provide a clearer picture of the threat landscape and boost cyber resilience across the UK's economy.

38. We welcome confirmation from the government that micro and small enterprises are exempt from the reporting requirements and small digital service providers can only be regulated if they are designated as a critical supplier in rare circumstances.

39. **We remain concerned about the feasibility for smaller organisations to meet the proposed two-stage reporting structure for cyber incidents as set out in the Bill, particularly requiring a full report to the relevant regulator and the NCSC within 72 hours.** While this would be feasible for larger organisations, this would not be the case for smaller supply chain companies and firms including smaller Managed Service Providers (MSPs) and critical suppliers, especially when investigations rely on external IT providers. **We want to see greater proportionality on these reporting requirements, with extended timelines or even an exemption for some smaller firms.** The reporting requirements could place further strain on outsourced IT and cybersecurity providers, who would likely be required to carry out potential investigations into incidents and prepare reports for multiple regulators on behalf of their smaller clients.

40. We would like to see clearer guidelines on what to report, and when, in recognition of the potential for the lack of cybersecurity expertise among businesses. Without appropriate guidance, businesses may have concerns about data privacy and be confused by the complexity of reporting thresholds.

41. The Bill requires the Secretary of State to produce a report at least every 5 years on how the legislation has been implemented, including exploring how the legislative objectives can be achieved in a less onerous regulatory provision. We recommend that these reviews are conducted on a more regular and timelier basis.

42. We welcome the publication of the government's Regulation Action Plan and support its wider ambitions to streamline regulation. It's important that these reporting requirements in the Cyber Security and Resilience Bill don't contradict the government's pledges to reduce regulation and duplication. The Financial Conduct Authority and the Bank of England will be shortly consulting on the regulation of Critical Third Parties, in parallel with the European Union's Digital Operational Resilience Act 2025 (DORA). Streamlined structures and coordination between the government and regulators are necessary to avoid

conflicting requirements and ensure effective resource allocation for intelligence agencies.

Ransomware

43. Ransomware is fast becoming the key cyber threat facing UK organisations. We work closely with the NCSC and last year developed a Ransomware Guide for organisations experiencing a ransomware attack. Our guide aims to minimise the impact of a ransomware incident, particularly on disruptions and costs to businesses, the number of ransoms paid, and size. Since its publication, our guide has been taken up internationally and endorsed by the Counter Ransom Initiative.

44. We submitted a response to the Home Office's consultation on its ransomware proposals earlier this year and have been closely engaging with government officials as those plans develop. We would like to have clarity on how the Bill's incident reporting requirements would be developed alongside the ransomware proposals being progressed by the Home Office, given how cyber security overlaps across several departments.

45. **We have serious concerns regarding the Home Office ransomware proposals.** We're concerned by the potential economic impact of introducing a targeted ban on ransomware payments and the development of a ransomware payment prevention regime covering the whole economy. **These proposals, while well intentioned, could lead to increased costs for businesses, business interruption, and potential insolvencies causing significant economic harm.** This is particularly acute for SMEs, which often lack both operational resilience and cyber insurance cover. Smaller firms simply can't withstand extended downtime, and without insurance or clarity on permissible actions, insolvency becomes a real risk.

46. These impacts can be mitigated by calibrating the details of the ransomware regime carefully. We look forward to continuing engaging with the government to achieve our shared ambitions to develop a ransomware regime that works for UK businesses and strengthens cyber security.

The Association of British Insurers
February 2026