Cyber Security and Resilience (Network and Information Systems) Bill

Memorandum from the Department of Science, Innovation and Technology to the Delegated Powers and Regulatory Reform Committee

1. INTRODUCTION

1. This memorandum has been prepared by the Department for Science, Innovation and Technology (DSIT) for the Delegated Powers and Regulatory Reform Committee, to assist with its scrutiny of the Cyber Security and Resilience (Network and Information Systems) Bill ('the Bill'). The Bill was introduced in the House of Commons on 12 November 2025. The memorandum identifies the provisions of the Bill which confer new powers to make delegated legislation. It explains in each case why the power has been taken and the nature of, and reason for, the procedure selected.

2. PURPOSE AND EFFECT OF THE BILL

1. The Bill will update the Network and Information Systems (NIS) Regulations 2018 ("the NIS Regulations") in order to better protect the essential and digital services that UK citizens and businesses rely on every day. The Bill will bring the NIS Regulations up to date by bringing more entities into scope, equip regulators with proportionate powers to better fulfil their duties, provide the government with sufficient powers to amend and add to the NIS Regulations in the future, and respond to threats to UK national security. These reforms will better safeguard the relevant network and information systems (the systems that allow computers and other devices to communicate with each other) of essential and digital services, and the suppliers they rely on, to ensure they are better defended against cyber attacks and more resilient if they are to suffer one.

2. The Bill is structured in 5 Parts and 2 Schedules.

3. The Bill includes measures to:
    a. Designate data centre operators as Operators of Essential Services (OESs) where UK data centre services provided are at or above 1 megawatt (MW) capacity, or, for services provided on an enterprise basis (which serve its own undertaking only), where the capacity is at or above 10MW. These data centre operators will be subject to duties as OESs. Ofcom and the Department for Science, Innovation and Technology will act as the joint regulator.
    b. Bring large load controllers, organisations that control 300MW of electrical load or more to remotely control consumer appliances, into scope of the NIS Regulations as OESs. The Department for Energy Security and Net Zero (DESNZ) and Ofgem will act as the joint regulator.
    c. Bring some managed service providers – referred to as Relevant Managed Service Providers (RMSPs) in the Bill – into scope of the NIS Regulations, to be regulated by the Information Commission (formerly the Information Commissioner's Office, or ICO). Those RMSPs in scope will be subject to the same duties as those placed on Relevant Digital Service Providers (RDSPs) already within scope of the NIS Regulations.

d. Grant the NIS regulators the power to designate and regulate organisations as "critical suppliers", if that organisation: provides goods or services to a provider of essential or digital services; the supplier relies on network and information systems for the purposes of that supply; and an incident affecting that supplier's network and information systems could cause disruption to essential or digital services who rely on them (or essential or digital services generally), and that disruption is likely to have a significant impact on the economy or day-to-day functioning of society in all or part of the UK.
e. Strengthen incident reporting requirements, by: expanding the definition of a reportable incident to also capture successful attacks that have compromised the integrity or security of a system, or could cause significant disruption in the future; introducing a two-stage reporting structure that will require regulated entities to notify their regulator of a significant incident no later than 24 hours after becoming aware of that incident, followed by a full report within 72 hours, as well as notifying the NCSC at both stages; and improving transparency by requiring RDSPs, RMSPs and data centre operators to alert customers who are likely to have been affected by a significant incident.
f. Introduce a new cost recovery framework to expand the options regulators have for recovering costs, allowing regulators to also recover the full costs associated with their NIS activities through a periodic fee. The use of this power will be underpinned by safeguards including transparency and consultation requirements.
g. Strengthen provisions to provide greater certainty on what information can be shared and with whom, to enable them to carry out their duties more effectively.
h. Strengthen regulators' ability to enforce the regulations. The maximum fine will be amended – enabling higher fines when appropriate – to reflect the significance of the regime and in line with comparable legislation. Penalty bands will also be simplified.
i. Enable the Secretary of State to designate a statement of strategic priorities to establish a unified set of expectations for the implementation of regulations, ensuring greater consistency of approach amongst the regulators who will have a duty to seek to achieve the objectives.
j. Future-proof legislation by providing the Secretary of State with powers to make regulations. This includes the ability to bring more sectors into scope of NIS Regulations, update and introduce security and resilience requirements for organisations within scope, and introduce supply chain risk management requirements.
k. Enable the Secretary of State to direct regulators or regulated entities to take proportionate action in response to actual or prospective threats that put the UK's national security at risk. Use of these powers will be subject to safeguards that directed action is necessary and proportionate.

3. DELEGATED POWERS

1. The delegated powers in the Bill are:

a. Part 3, Chapter 1: Introductory

i. **Clause 24(3): Key definitions in Part 3 ("essential activity"):** this power allows the Secretary of State to make regulations to specify an activity as an "essential activity".

ii. **Clause 24(6): Key definitions in Part 3 ("regulatory authority"):** this power allows the Secretary of State to make regulations to designate a person as a "regulatory authority".

b. **Part 3, Chapter 3: Regulations about security and resilience of systems**

i. **Clause 29(1): regulations relating to security and resilience of network and information systems:** This power allows the Secretary of State to make regulations for the purposes of identifying, managing and reducing the risk of, as well as mitigating and reducing adverse impacts resulting from, security or operational compromises in relation to relevant network and information systems.

ii. **Clause 32(5): provision about financial penalties:** This power allows the Secretary of State to amend the maximum penalty amounts specified in Clause 32(3)(a)(i) or (b), for the purposes of reflecting inflation.

c. **Part 3, Chapter 4: Code of practice**

i. **Clause 37(7): procedure for issue of code of practice:** This power allows the Secretary of State to amend the procedure for issuing or reissuing a code of practice describing how regulated persons can comply with the requirements imposed by regulations made under Clause 29(1).

d. **Part 3, Chapter 5: Report on network and information systems legislation**

i. **Clause 40(5):** This power relates to the requirements for the Secretary of State to report on the NIS Regulations (as amended by this Bill), any regulations made under any provision of Chapter 1 or 3 of Part 3, and Part 3 and Part 4 of the Bill itself. It allows the Secretary of State to amend requirements on what the report must contain.

e. **Part 4: Directions for National Security Purposes**

i. **Clause 49(5): penalty amounts:** This power is in the form of a duty which requires the Secretary of State to make provision by regulations to define what is meant by an "undertaking" and determine how an undertaking's turnover is to be determined, for the purposes of determining an appropriate penalty for non-compliance with a direction given under Clause 43.

ii. **Clause 49(7) penalty amounts:** This power enables the Secretary of State to make regulations to amend the maximum penalty amounts for non-compliance with a direction for the purpose of reflecting inflation.

f. Part 5: General

i. **Clause 60(3): commencement:** This power enables the Secretary of State to commence the majority of the provisions of the Bill by regulations, apart from those listed by Clause 60(1) and (2).

ii. **Clause 60(7): transitional arrangements:** This power enables the Secretary of State to make transitional or saving provision in connection with any provision of this Act.

4. ANALYSIS OF DELEGATED POWERS BY CLAUSE

Part 3, Chapter 1: Introductory

Clause 24(3): Key definitions in Part 3 ("essential activity")

Power conferred on: Secretary of State

Power exercised by: Regulations (Statutory Instrument)

Parliamentary Procedure: affirmative procedure

Context and purpose

1. Clause 24(3) allows the Secretary of State to make regulations to specify an activity as an "essential activity" for the purposes of Part 3 of the Bill.
2. The purpose of this power is to enable the government to both bring new types of activities into scope and amend existing definitions of such "activities" in scope for the purposes of this Part, which includes the regulations made under Clause 29(1). The power can only be used to specify activities which are considered to meet the criteria set out in Subsection (4), namely that the activity is essential (i) to the economy of the whole or any part of the UK; or ii) to the day to day functioning of society in the UK or any part of the UK. Subsection (5) makes clear that an activity can include the provision of service and that references to "essential activity" elsewhere in the Bill are to be construed accordingly.
3. The clause is designed to maintain a high bar for broadening the scope of the regulatory framework by restricting inclusion to those activities (including services) which are essential to the running of UK society or the functioning of our economy. This meets the government's key objective of protecting the activities that the public and businesses rely on every day and protecting the economy from harm, without imposing undue burden on businesses.

Justification for taking the power

4. This power is necessary to ensure that entities that are fundamental to the functioning of the UK economy and society can be brought in scope of the NIS Regulations, or other cyber security regulations made under Clause 29(1). It is necessary to create this power now via this Bill because the government no longer has the appropriate powers to bring new entities into scope of the NIS Regulations, following the repeal of the European Communities Act 1972.

5. Without an appropriate power to update them, the NIS Regulations have become outdated as the types of services that we rely upon, as well as the cyber threat landscape, have evolved. This concerns both new and emerging sectors and services, as well as existing sectors covered by the NIS Regulations, definitions for which have fallen out of date due to the passage of time and advancement of technology. A delegated power acknowledges that what is fundamental will change over time, making it impractical to list services or activities in primary legislation without the power to amend or add to them. This power ensures the NIS Regulations can be amended to keep pace with the emergence of new critical services and other activities that are driven by technological change or market evolution. It will also accommodate activities in sectors which are not currently regulated, but which may need to be reprioritised due to changing assessments of their criticality and risk profile.

6. For example, the Bill recognises the increasing importance of data centres to our digital lives, as well as load controllers as facilitating smart, flexible energy solutions, by bringing both sectors into scope of the NIS Regulations. This delegated power will enable government to bring more entities into scope in the future without being beholden to the timescales of primary legislation. Considering the lead-in time for compliance with cyber security regulations, speed is fundamental in ensuring that the economy and security of the nation is preserved and services are secured against threats.

Justification for the procedure

7. The requirement for regulations to undergo the affirmative procedure (per Clause 42(5)(a)) will ensure significant parliamentary scrutiny and oversight. This is appropriate because the added regulation will have a direct impact on the services and activities in question, and full parliamentary debate and scrutiny is required to ensure the power is used proportionately and effectively.

8. Clause 42(1)(a) requires the Secretary of State to consult such persons as the Secretary of State considers appropriate before making the regulations under this power. This requirement is included to ensure that organisations that are likely to be impacted by inclusion under the regulations have an opportunity to provide feedback and to inform the decision, where appropriate, in order to ensure transparency.

Clause 24(6): Key definitions in Part 3 ("regulatory authority")

Power conferred on: Secretary of State

Power exercised by: Regulations (Statutory Instrument)

Parliamentary Procedure: affirmative procedure

Context and purpose

9. Clause 24(6) allows the Secretary of State to make regulations to designate a person as a “regulatory authority” for the purposes of this Part, which includes regulations made under Clause 29(1). Subsection (7) sets out that a person can only be designated as such if they exercise functions of a public nature.

10. The purpose of this power is to enable government to designate appropriate regulators to support and monitor the compliance with the NIS Regulations from those entities in scope, as amended by this Bill or via regulations made under powers provided for in this Bill.

Justification for taking the power

11. A regulatory regime requires regulatory authorities to supervise, provide advice, enforce, and implement the legislation. For the entities already in scope of the NIS Regulations, there are already regulatory authorities (regulators) tasked with monitoring their compliance – for example, online marketplaces are regulated by the Information Commission. However, for new entities brought into scope by virtue of Clause 24(3), it is essential that an appropriate regulator is assigned. Where an existing regulator does not have the appropriate expertise, a new regulator may need to be designated.

12. Regulators are sector-specific and hold substantial expertise in the particular area that they are designated to regulate. As the sectors in scope of the NIS Regulations evolve (as allowed for by Clause 24(3)), so too should the regulators. This power also enables the Secretary of State to respond to any structural or legal changes in the status of existing regulatory authorities, as well as to the creation of new ones, should this be deemed necessary.

Justification for the procedure

13. The requirement for regulations to undergo the affirmative procedure (per Clause 42(5)(a)) will ensure significant parliamentary scrutiny and oversight.

14. Clause 42(1)(b) requires the Secretary of State to consult such persons as the Secretary of State considers appropriate before making the regulations under this power. This requirement is included to ensure that organisations that are likely to be impacted by virtue of being designated as a regulator, or by being regulated by that entity, have an opportunity to provide feedback and to inform the decision, where appropriate. This will contribute to transparency and predictability.

Part 3, Chapter 3: Regulations about security and resilience of systems

Clause 29(1): Regulations relating to security and resilience of network and information systems

Power conferred on: Secretary of State

Power exercised by: Regulations (Statutory Instrument)

Parliamentary Procedure: affirmative procedure in the cases listed in Clause 42(2), otherwise negative procedure

Context and purpose

15. Clause 29(1) grants the Secretary of State the power to make regulations for the purposes of, or in connection with:
    a. Identifying, managing and reducing the risks in relation to relevant network and information systems;
    b. Mitigating and reducing adverse impacts resulting from such security or operational compromises; or
    c. Strengthening the resilience of network and information systems and the security of the physical environment in which such systems are housed.

16. "Security or operational compromises" are given meaning by provisions in Clause 29(5). It establishes that "security or operational compromises" are anything that compromises certain listed aspects in relation to relevant networks and information systems, such as confidentiality, integrity, availability, operation, authenticity, or unauthorised access and interference, among others.

17. "Relevant network and information systems" is given its meaning under Clause 29(3). It provides that a relevant information system is one used or relied on in connection with the carrying on of a specified essential activity or an activity-critical supply. It includes any associated systems.

18. An "activity-critical supply" is defined at Clause 29(5) as a supply of goods or services without which the carrying on of a specified activity would be at risk of disruption.

19. Clauses 30 to 34 provide more detail on what the Cyber Security Regulations made under Clause 29(1) may contain.

    i. Clause 30(1) provides that regulations may impose requirements on "regulated persons". The meaning of this term is explained in Subsections (2) to (5). It includes an OES, an RDSP, an RMSP, a critical supplier (all within the meaning of the NIS Regulations) or a person, or a person of a description, specified in regulations made under clause 29(1). The Secretary of State may specify persons (whether or not established in the UK) who carry on essential activities (including the provision of services) in the UK (as defined in Clause 24(3)) or who provide an "activity-critical supply". They can also provide for a regulatory authority to designate a regulated person. Subsection (6) sets out a non-exhaustive list of sorts of requirements than can be imposed on regulated persons.

    ii. Clause 31 provides that regulations may confer functions on regulatory authorities in connection with: monitoring compliance; investigating suspected non-compliance (including inspections and other evidence-gathering, tests and interviews); securing compliance (including issuing penalties and their amounts); and mitigating the effect of non-compliance. Subsection (3) expands on what these duties may entail, although the list is non-exhaustive. As the power can be used to make provision for financial penalties, Subsection (6) contains an important safeguard which ensures that regulations containing such provision must also include provision for appeals.

iii. Clause 32 sets out that where the regulations make provisions for the imposition of financial penalties, the regulations may specify the amount or provide for: how the amount will be determined; how penalties will be received; and how regulators will recover unpaid penalties. Clause 32 sets out that the power under Clause 29(1) can be used to increase maximum penalties for non-compliance, but includes safeguards so that the maximum penalty payable by an undertaking cannot exceed 10% of annual turnover or £17 million, whichever is highest, and, in the case of a non-undertaking, £17 million. Any use of the delegated power to increase the maximum penalties payable by an undertaking up to 10% is also subject to the affirmative procedure.

iv. Clause 33(1) specifies that regulations may confer functions on regulatory authorities in connection with information sharing and restriction on such information disclosure. It also sets out that regulations may confer functions in connection with issuing guidance, record keeping, conducting reports and reviews, and consultation and cooperation with other persons (including persons outside the UK). Subsection (4) sets out that regulations may designate persons other than regulatory authorities for the purposes of exercising functions conferred by the regulations, as long as they exercise functions of a public nature. A non-exhaustive list of these functions is set out at Subsection (5).

v. Clause 34 specifies that regulations may make provision for a regulatory authority to impose fees or other charges on regulated persons in respect of costs incurred in the exercise of functions under the regulations.

20. The purpose of this power is to enable the government to update the NIS Regulations without requiring an Act of Parliament. As set out further in the justification below, this is crucial for ensuring government can respond to new and evolving cyber threats which circumvent the current NIS Regulations, without being beholden to the timeframes of primary legislation.

<u>Justification for taking the power</u>

21. Following the revocation of the European Communities Act 1972, the government no longer has the power to update the NIS Regulations to ensure they effectively and appropriately support the cyber security and resilience of those carrying out activities which are essential to the functioning of society in the UK or the UK economy. This has meant that the UK's cyber security and resilience has weakened as the frequency and sophistication of attacks have amplified. UK citizens pay the price for these attacks, whether this be from disrupted public services or an unstable business environment which undermines economic growth. In 2024, a ransomware attack on a key supplier to the NHS led to over 11,000 postponed acute outpatient appointments and elective

procedures. In the same year, cyber criminals targeted a managed service provider (MSP) providing payroll services to the Ministry of Defence, exposing the records of 27,000 military personnel, reservists and veterans. Despite an understanding that unregulated MSPs and increasingly complex supply chains are putting essential public services at risk, the government has been unable to take significant steps to strengthen the NIS Regulations against this threat, except by introducing this primary legislation. New vulnerabilities will undoubtedly emerge in the future, and the government must have an appropriate mechanism to strengthen the NIS Regulations in a timely manner.

22. The attack on the Ministry of Defence also demonstrates the impact of outdated regulations on the UK's national security. Without a mechanism to update the NIS Regulations, the situation will only worsen and be exploited by criminals and state actors. The UK is the most targeted country in Europe for cyber attacks, and we know that state-sponsored actors are posed to disrupt our services and way of life, as they have done elsewhere. Chinese state-sponsored threat actors have already targeted US critical sectors. For example, Volt Typhoon is a cyber threat acting on behalf of China and has targeted energy, transport and water sectors in the US, and could be laying the groundwork for future disruptive and destructive cyber attacks. Relying on primary legislation to make vital changes to respond to such threats in an increasingly changing technology and threat environment is so impractical that it could be considered dangerous. We must ensure that government can respond swiftly to emerging threats in a way that is robust and proportionate.

23. This power is therefore needed to enable the government to update our vital cyber regulations so that they can respond effectively to current and future circumstances and needs. Evolving technology, cyber risks and business models will all have a bearing on what kinds of processes regulated organisations will need to put in place, what kind of oversight regulators will need to provide and what types of enforcement processes are necessary to ensure compliance. This power sufficiently recognises the changing nature of the cyber security landscape, without granting the government disproportionate powers in this space. That is because the regulations are constrained by the set parameters and purposes clauses, ensuring they can only be used to address these challenges. DSIT is confident that the power is necessary and proportionate to the cyber security threats facing the UK, and consistent with delegated powers in legislation dealing with fast-moving technology.

<u>Justification for the procedure</u>

24. Clause 42 imposes a duty on the Secretary of State to consult such persons as the Secretary of State considers appropriate in certain cases before making regulations under Clause 29(1). This requirement applies to regulations which make provision by virtue of the provisions of the Bill listed in Clause 42(2) (see paragraph 27 below). This will ensure that the appropriate stakeholders are consulted and viewpoints considered before regulations are made.

25. Where there is a requirement to consult, the regulations will be made via the affirmative procedure, per Clause 42(5)(a). The affirmative procedure is also required where

regulations amend primary legislation (42(5)(b)); this concerns only consequential, supplementary, incidental, transitional or saving provisions. The overarching principle behind the requirements is that changes to the regulations should require appropriate consultation and the affirmative procedure, except in cases where the change is purely procedural.

26. As such, the Secretary of State will consider appropriate consultation ahead of the affirmative procedure where the regulations concern:

    i. Duties imposed on regulated persons (defined by Clause 30(2)), as per Clause 30(1), except for regulations that set the process for a person being designated by a regulatory authority;

    ii. Functions on regulatory authorities, per Clause 31(1);

    iii. Provisions about appeals to a court or tribunal against a penalty or a direction, per Clause 31(6), except for provisions described in Clause 31(7)(b) (procedure for making an appeal);

    iv. Provisions about the disclosure of information per Clause 33(1)(a), except for provisions described in Clause 33(2)(b) (the form or manner in which a requirement to provide information may be imposed);

    v. Functions conferred on persons who exercise functions of a public nature, other than regulatory authorities, for the purposes of exercising functions conferred by the regulations, per Clause 33(4); and

    vi. Provision for a regulatory authority to impose fees on regulated persons, per Clause 34.

27. Where regulations make provisions which do not fit into the criteria set out above which are likely to be procedural or clarificatory in nature, the negative procedure will be followed.

Clause 32(5): provision about financial penalties (reflecting inflation)

Power conferred on: Secretary of State

Power exercised by: Regulations (Statutory Instrument)

Parliamentary Procedure: negative procedure

<u>Context and purpose</u>

28. Clause 32 sets out that where regulations made by virtue of Clause 29(1) provide for regulatory authorities to impose financial penalties for non-compliance, the regulations must specify an amount of penalty or provide for how the amount will be determined. Clause 32 sets out that the power under Clause 29(1) can be used to increase maximum penalties for non-compliance, but includes safeguards so that the maximum penalty payable by an undertaking cannot exceed 10% of annual turnover or £17 million, whichever is highest, and, in the case of a non-undertaking, £17 million. The power in Clause 32(4) allows the Secretary of State to, by regulations, amend the

amount specified in Clause 32(3)(a)(i) or (b) (£17 million) for the purpose of reflecting inflation.

29. The purpose of this power is to enable the government to ensure that the maximum penalty for non-compliance with the regulations is not rendered irrelevant and ineffective, either because it is set too low to have no deterrent effect, or because of inflation.

Justification for taking the power

30. This power is necessary to ensure that penalties for non-compliance remain proportionate and effective in the long-term. It is crucial that the mechanisms for enforcing the regulations act as an impactful deterrent, without which it is not guaranteed that the regulations will be adhered to by the organisations in scope. Widespread non-compliance, or even inconsistent compliance, will undermine the objectives of the regulations, which are to reduce the risk of and mitigate the effects of cyber attacks on essential and digital services, the compromise of which can have a devastating impact on public safety, national security and the wider economy.

Justification for the procedure

31. To exercise this power will require the use of the negative procedure. This is proportionate to the limitation in the power which specifies that any amendments to the maximum penalty are for the purpose of reflecting inflation. This means that the power cannot be used for significant policy changes on penalties for non-compliance. As such, we consider the negative procedure to provide an appropriate level of scrutiny for the exercise of this power.

Part 3, Chapter 4: Code of Practice

Clause 37(7): procedure for issue of a code of practice

Power conferred on: Secretary of State

Power exercised by: Regulations (Statutory Instrument)

Parliamentary Procedure: affirmative procedure

Context and purpose

32. Clause 36 specifies that Secretary of State may issue a code of practice for regulated persons to aid understanding and compliance of the duties imposed by them under NIS Regulations and regulations made under Clause 29(1). Clause 37 describes the procedure, including a requirement for Secretary of State to lay a draft of the code in Parliament. Clause 37(7) enables Secretary of State to change the procedure for issuing or reissuing a code by amending Clause 36 so far as it relates to consultation and Clause 37 (except Subsection (7)).

33. The purpose of this power is to allow the government flexibility on the procedure for issuing a code of practice. This approach has been taken to prioritise the content of the code of practice, rather than arbitrary requirements. For example, if a 40-day period

for Parliament to consider the draft becomes unfeasible and is a detriment to the quality and usefulness of a code, this power enables government to take practical steps to remedy this. Or, as another example, a Secretary of State may choose to amend Clause 36(3) to require consultation of particular people for future iterations of the code of practice.

Justification for taking the power

34. As set out in its purpose, the power is necessary to ensure the requirements for publishing a code of practice are not so rigid as to hamper its usefulness. The purpose of a code is to provide practical guidance for persons seeking to comply with the regulations. If the procedure is so rigid as to hamper this objective, then it would be a counterproductive exercise. Retaining an ability for government to respond and reflect on the process will ensure the code of practice remains a helpful tool for regulated persons.

Justification for the procedure

35. As set out in Clause 42(5)(b) this power is subject to the affirmative procedure. This will enable the appropriate parliamentary scrutiny where the Secretary of State is seeking to amend the reporting requirements, to ensure that Parliament is able to properly scrutinise the report that is laid before it.

Part 3, Chapter 5: Report on network and information systems legislation

Clause 40(5): Report on network and information systems legislation

Power conferred on: Secretary of State

Power exercised by: Regulations (Statutory Instrument)

Parliamentary Procedure: affirmative procedure

Context and purpose

36. Clause 40 requires the Secretary of State to lay in Parliament, as well as publish, a report on the operation on cyber security legislation during the review period per Subsection (2). Clause 40(5) grants the Secretary of State the power to amend Clause 40 via regulations, so long as it concerns the matters to be covered in the reports. It replicates existing provisions contained in Regulation 25 of the NIS Regulations (which the Bill revokes).

37. Clause 40(4) outlines what the report must include, including setting the objectives for the legislation, assessing to what extent they have been met, and what uses of the power to make delegated legislation (per Clause 29(1)) have been made.

38. The purpose of this power is to allow the government flexibility on the content of the report. This is to ensure the appropriate content is covered in the reports, recognising that this may change and be expanded upon over time. For example, a particular report may cover aspects additional to what is listed in Subsection (4) which are found to be

useful. Here, the Secretary of State may wish to amend Subsection (4) to mandate that those aspects are included in future reports.

Justification for taking the power

39. As set out in its purpose, the power is necessary to ensure the reporting requirements are not so rigid as to hamper their usefulness. The report is meant to ensure that the impact of cyber security legislation is clearly assessed, scrutinised by Parliament, and publicly understood, to ensure transparency and accountability for the government. Retaining an ability to the contents of the review will allow the government to respond and reflect on feedback from both Parliament and the wider public, ensuring that the report covers all necessary aspects and is as comprehensive as possible.

Justification for the procedure

40. As set out in Clause 42(5)(b), this power is subject to the affirmative procedure. This will enable the appropriate parliamentary scrutiny where the Secretary of State is seeking to amend the reporting requirements, to ensure that Parliament is able to properly scrutinise the report that is laid before it.

Part 4: Directions for National Security Purposes

Clause 49(5): penalty amounts

Power conferred on: Secretary of State

Power exercised by: Regulations (Statutory Instrument)

Parliamentary Procedure: negative procedure

Context and purpose

41. Clause 43 enables the Secretary of State to give a direction to a regulated person in the interests of national security. Subsection (3) provides for what requirements a direction may impose, but the list is non-exhaustive, as long as the direction meets the national security criteria outlined in Subsection (1). Per Subsection (5), the direction is compulsory and must be complied with. Clause 49 enables the Secretary of State to impose a penalty on the regulated person if they have not complied with the direction. Where the person is an undertaking, the penalty amount may not exceed £17 million or 10% of the undertaking's turnover, whichever is higher. Where a person is not an undertaking, the penalty amount cannot exceed £17 million. The power in Clause 49(5) requires the Secretary of State to make regulations to define "undertaking" and to determine the turnover of a person for purposes of determining the penalty amount for non-compliance with a direction.

42. The purpose of this power is to ensure that regulated persons found to be in breach of a Secretary of State direction are liable for a penalty fine of the appropriate amount. Setting out the parameters in scope of the 10% fine in regulations better enables technical distinctions to be made, with the end objective of a proportionate fine being imposed on the contravening party.

Justification for taking the power

43. The inclusion of a power for the Secretary of State to specify these definitions in regulations is the correct approach because the definitions are technical. It also ensures the penalties in the regime stay up-to-date and are calculated appropriately. This is of particular importance because the secondary legislation will likely refer to certain accounting principles that may change from time to time. This power follows precedent set by the Digital Markets, Competition and Consumers Act 2024 (Section 90), whereby the definition of turnover is set out in regulations.

Justification for the procedure

44. A negative procedure is proportionate for regulations that are of a technical and non-controversial nature. This follows the precedent set by the Digital Markets, Competition and Consumer Act 2024.

Clause 49(7): penalty amounts

Power conferred on: Secretary of State

Power exercised by: Regulations (Statutory Instrument)

Parliamentary Procedure: negative procedure

Context and purpose

45. In addition to the penalties set out in paragraph 42, Clause 49 enables the Secretary of State to impose a penalty for non-compliance with a direction on a regulated person that is not an undertaking. The penalty amount may not exceed £17 million (Subsection (2)(b)). For continuing non-compliance with a direction, the Secretary of State may impose daily penalties of up to £100,000 per day (Subsection (3)(a)).

46. Clause 49 also enables the Secretary of State, or a regulatory authority that is responsible for monitoring compliance with a direction under Clause 45, to impose a penalty on a regulated person if they have not complied with an information request issued in line with Clause 46. The penalty amount may not exceed £10 million (Subsection (2)(c)) or, in the case of a continuing contravention, £50,000 per day (Subsection (3)(b)).

47. The power in Clause 49(7) enables the Secretary of State to make regulations to amend the maximum penalty amounts in Subsections (2) and (3) for the purpose of reflecting inflation.

48. The purpose of this power is to ensure that regulated persons found to be in breach of a direction, or information request, are liable for a penalty fine of the appropriate amount, and what is an appropriate maximum amount will change over time because of inflation.

Justification for taking the power

49. The inclusion of a power for the Secretary of State to amend these amounts in regulations is the correct approach because any adjustments will be limited to being in

line with inflation, therefore limiting misuse of the power, and the calculation of inflation is technical. It also ensures the penalties in the regime continue achieving the aim of encouraging compliance.

Justification for the procedure

50. A negative procedure is proportionate for regulations that are of a technical and non-controversial nature.

Part 5: General

Clause 60(3): Commencement

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: None

Context and purpose

51. Clause 60(3) grants the Secretary of State to bring certain measures in this Act into force through regulations.

Justification for taking the power

53. This is a standard clause for commencing the provisions of an Act. Enabling certain provisions to be brought into force via regulations will afford the necessary flexibility to commence the provisions at an appropriate time. This allows the government to have regard to the need to conduct any necessary consultation, make secondary legislation, issue guidance and put the necessary procedures in place to support implementation.

Justification for the procedure

54. As is usual for commencement powers, regulations made under Clause 60 are not subject to any parliamentary procedure. Parliament has approved the principle of the provisions to be commenced by enacting them. Commencement by regulations enables the provisions to be brought into force at the time best suited to the sector.

Clause 60(7): transitional provisions

Power conferred on: Secretary of State

Power exercised by: Regulations

Parliamentary Procedure: None

Context and purpose

55. Clause 60(7) grants the Secretary of State the power to make transitional or saving provision in connection with the coming into force of any provision of this Act. Subsection 8 enables the Secretary of State to make different provisions for different purposes under this Act.

Justification for taking this power

56. This is a standard clause for enabling transitional provision or saving provision in connection with the coming into force of any provision of this Act.

Justification for the procedure

57. As is common for powers to make transitional provision in respect of the coming into force of an Act, regulations made under Clause 60 are not subject to any parliamentary procedure.

Department Name: Department for Science, Innovation and Technology

Date: 12 November 2025