Cyber Security and Resilience Bill

Lead department	Department for Science, Innovation and Technology
Summary of proposal	The proposal is to update the Network and Information Systems (NIS) Regulations 2018 to strengthen the cyber security and resilience of more types of services, fixing vulnerabilities stemming from large gaps of current NIS coverage. It will do this by bringing more entities, sectors and services into scope.
Submission type	Options Assessment – 20th May
Legislation type	Primary legislation
Implementation date	TBD
RPC reference	RPC-DSIT-25054-IA (1)
Date of issue	18 July 2025

RPC opinion

Rating[1]	RPC opinion
Fit for purpose	The Department evidences the problem under consideration. The IA identifies a sufficient range of long-list options and justifies the selection of the short-list option. The Department explains that whilst this diverges from Green Book guidance, this is appropriate due to the number of measures in the Bill. The IA clearly explains the reasoning behind this and justifies why other long-list options are not viable for short-list appraisal using critical success factors. The IA has identified and monetised the key impacts from the proposal and outlines the key reasons for selecting the preferred option compared to the 'do-nothing' option.

[1] The RPC opinion rating is based only on the robustness of the rationale, options identification (including SaMBA) and justification for preferred way forward, as set out in the Better Regulation Framework guidance. RPC ratings are fit for purpose or not fit for purpose.

RPC summary

Category	Quality[2]	RPC comments
Rationale	**Green**	The IA outlines and evidences the problem under consideration. The IA could further utilise PIRs to evidence how the regulations are outdated in other areas. The IA's argument for intervention is focused on the existence of market failures.
Identification of options (including SaMBA)	**Green**	The IA identifies a sufficient range of long-list options but could benefit from using the Green Book's Strategic Options Framework Filter (SOFF). The IA provides sufficient justification for discarding options from the long-list, assessing all long-list options against critical success factors (CSFs). The IA provides a sufficient SaMBA, exempts SMBs from the regulations except for when designated as a critical supplier.
Justification for preferred way forward	**Green**	The IA has identified and monetised the key impacts from the proposal and conducts break-even analysis to indicate the scale of potential benefits. The IA could benefit from further explaining some of the assumptions. The IA outlines the key reasons for selecting the preferred option compared to the 'do-nothing' option.
Regulatory Scorecard	**Satisfactory**	Despite a negative NPSV, the proposal is expected to have a positive impact to total welfare and business, due to non-monetised benefits to society from a reduction in cyber attacks. The IA could benefit from setting out the calculations underpinning the EANDCB metric calculation and further considering distributional impacts. The Department sufficiently considers the impact of the proposal on wider government priorities.
Monitoring and evaluation	**Satisfactory**	The Department outlines the data sources which will be used to underpin this review, explaining their limitations. The OA could benefit from including further detail on the nature of this qualitative and quantitative data and how it will be gathered.

[2] The RPC quality ratings are used to indicate the quality and robustness of the evidence used to support different analytical areas. The definitions of the RPC quality ratings can be accessed here.

Response to initial review

As originally submitted, the OA was not fit for purpose as the IA did not provide sufficient justification for discarding options from the long-list and needed to further justify why other long-list options have not been carried forward to the short-list. Due to the large number of measures within the Bill, the RPC considered that it may not be appropriate to include further short-list options across all measures, but the IA needed to clearly explain the reasoning behind this, justifying why the other long-list options are not viable for short-list appraisal.

The Department has provided sufficient justification for discarding options from the long-list, assessing all long-list options against critical success factors (CSFs). The Department explains that whilst this diverges from Green Book guidance (to have multiple options in the short-list), this is appropriate due to the number of measures in the Bill and as this option has been announced as part of the package of measures in the King Speech. The IA clearly explains the reasoning behind this and justifies why other long-list options are not viable for short-list appraisal.

Summary of proposal

The Cyber Security and Resilience Bill ('the Bill') will strengthen the UK's cyber defences, safeguard our critical infrastructure and better protect more businesses than ever from costly cyber attacks in a way that does not overburden them. It will do this by amending the Network and Information Systems (NIS) Regulations 2018 by bringing more entities, sectors and services into scope, empowering regulators to drive compliance and equipping government to take decisive action to protect our national security.

The IA has considered the following short-list options:

- **Option 1**: Do nothing
- **Option 2**: Primary legislation. The proposed measures are:
    1. Bring managed service providers (MSPs) into scope of the NIS Regulations.
    2. Bring data centres at or above 1MW capacity and enterprise data centres at or above 10MW capacity into scope of the NIS Regulations.
    3. Introduce load control as an essential service in the electricity sector and bring large load controllers (those with a potential aggregate load of 300MW or above) in scope of NIS Regulations.
    4. Enable regulators to identify and designate specific high-impact suppliers as 'designated critical suppliers', bringing them under comparable obligations as operators of essential services (OESs) and relevant digital service providers (RDSPs).
    5. Improve incident reporting by expanding the incident reporting criteria, updating incident reporting times, streamlining how information is shared with the national cyber security centre (NCSC), and enhancing transparency requirements for RDSPs, MSPs being brought into scope, and data centres.

6. Strengthen information sharing provisions, such as by providing a clear gateway for regulators to share information with public authorities, and vice versa.
7. Expand the duty in secondary legislation on RDSPs to provide information to the Information Commissioner's Office (ICO) to enable them to take a more proactive approach to assessing the risk of RDSPs and MSPs being brought into scope.
8. Improving cost recovery by enabling the full costs of NIS-related functions to be recoverable through flexible cost recovery mechanisms.
9. Grant the Secretary of State the power to designate a Statement of Strategic Priorities.
10. Grant the Secretary of State powers to update the regulatory framework in the future.
11. Enable the Secretary of State to update existing technological and methodological security requirements, via secondary legislation.
12. Enable the government to set stronger supply chain duties for OESs and RDSPs in secondary legislation.
13. Grant the Secretary of State the power to direct regulated entities to take action to address threats and incidents, when it is necessary and proportionate for national security.
14. Grant the Secretary of State the power to direct regulators to take action, when it is necessary and proportionate for national security.

The IA presents an NPSV of -£1,201m for the preferred option, with an EANDCB of £137.7m. This is largely driven by costs incurred by newly regulated entities for meeting the requirements regulations, including physical and cyber security costs, incident reporting costs and contract change costs.

Rationale

Problem under consideration

The IA outlines the problem under consideration, explaining how cyber attacks are becoming more frequent and sophisticated, whilst the current legislation (NIS Regulations 2018) is considered to be outdated. The Department evidences this problem, referencing the number (and case studies) of significant cyber incidents, and the associated loss faced by businesses and critical suppliers, such as the NHS.

The IA also provides evidence to illustrate why they consider the regulations to be outdated, referencing the 2022 PIR which found a low level of reported incidents due to the narrow definition of a 'significant incident'. The Department could further explain the incentives behind setting this original definition in the regulations, considering why this definition has become out of date. This could help to set the scene for why this is no longer effective and justify the need for intervention. The IA could also be improved by further evidencing how the regulations are outdated in other areas, clearly setting out what the current scope is under the existing regime and how this relates to the identified problems. This would help the Department to show how the proposal will solve for the problem under consideration.

Argument for intervention

The IA's argument for intervention is focused on the current regulatory inflexibility. The IA also uses the existence of market failures to form its argument for intervention, referencing positive externalities, information asymmetry and coordination failure. The IA would be improved by providing relevant evidence to support these arguments. The IA could also expand on its argument of imperfect information, further explaining how cyber security information is incomplete for businesses.

Objectives and theory of change

The IA sets out the overarching SMART objectives for the proposal, as well as the objectives for each individual measure. However, the Department would benefit from fully applying the SMART objectives framework when forming the objectives. The provided objectives focus on policy outcomes and are achievable and realistic but do not consider the specific, measurability and time-limited aspects of the SMART framework.

The theory of change diagram, although fit for purpose, could more clearly show the causal mechanisms linking inputs,activities and the final outcomes of the interventions.

Identification of options (inc. SaMBA)

Identification of the 'long-list' of options

The IA identifies a sufficient range of long-list options to strengthen the UK's cyber defences, setting out a set of long-list options for all fourteen measures within the proposal. These include options to enable regulators to designate 'critical suppliers', the Department to designate 'critical suppliers', as well as options for expanding the reporting criteria or requiring all incidents to be reported. The Department details these options in the IA, describing qualitatively what they would involve and their associated risks. However, the IA could benefit from further explaining how some options would work in practice, such as outlining how the options to bring MSPs, data centres and large load controllers into scope would change their day-to-day operations. The assessment could also be improved by including detail on the process behind developing the long-list of options, such as how research and other evidence have been used to form these policies. The long-list of options could benefit from using the Green Book's Strategic Options Framework Filter (SOFF), which could help present the long-list in greater detail whilst retaining a clear and concise structure.

Consideration of alternatives to regulation

The Department discusses non-regulatory policy alternatives for each measure, such as encouraging the use of voluntary cyber standards and guidance and developing education and awareness campaigns. The IA explains why these options are not suitable, as they have not been effective at solving the market failure previously. These options have also received a negative response when tested in a call for

views. However, the IA could consider implementing these options in combination with the regulatory intervention.

Justification for the short-listed options

The IA provides sufficient justification for discarding options from the long-list, assessing all long-list options against critical success factors (CSFs). The Department uses the CSFs to shed light on the options strategic fit, effectiveness and feasibility, and demonstrates that one long-list option is viable for each measure. When taken together this constitutes the shortlisted option (in addition to the do-nothing option), primary legislation. This assessment justifies the selection of this short-list option, and the Department explains that whilst this diverges from Green Book guidance (to have multiple options in the short-list), this is appropriate as this option has been announced as part of the package of measures in the King Speech. Furthermore, due to the large number of measures within the Bill, it has not been considered appropriate to include further short-list options across all measures. The IA clearly explains the reasoning behind this and justifies why other long-list options are not viable for short-list appraisal. However, the Department's use of CSFs could be improved, and the IA could benefit from aligning the CSFs with the specific factors as set out in the Green Book.

SaMBA and medium-sized business (MSB) assessment

The IA provides a sufficient SaMBA. The proposal exempts SMBs from the regulations, as in the previous NIS regulations (2018). The IA justifies this exemption, explaining that firms with the largest externalities from their cyber risk are the medium and large firms covered by the NIS Regulations, as these are the firms with the largest number of customers. To regulate all services provided by small and micro MSPs would be disproportionate, as many do not pose serious vulnerabilities.

This exemption does not apply to SMB RDSPs who can be designated as a 'critical supplier' by their regulator as part of the new regulations. The IA explains that this modification is necessary as all critical suppliers, regardless of size can pose a risk to critical national infrastructure and form part of essential supply chains. This modification is also supported by the Federation of Small Business and responses from a 2022 consultation. The IA could benefit from setting out any potential impact from this modification on these SMBs and considering if the impacts will be disproportionate. The IA states that the Department will ensure appropriate guidance is designed for these SMBs now captured by the regulations but could provide further detail on this mitigation.

Justification for preferred way forward

Identifying impacts and scale

The Department has identified and monetised the key impacts from the proposal, estimating an NPSV of -£1,201m for the preferred option. The main costs are those incurred by newly regulated entities for meeting the requirements regulations, including physical and cyber security costs, incident reporting costs and contract change costs. The IA has used internal analysis,engagement with stakeholders and

research from Frontier Economics to identify the number of newly regulated firms in scope. Existing regulated firms will also face incident reporting costs due to the expanded reporting introduced by the regulations, as this may require an organisation to have staff on weekends. The IA could benefit from providing more detail on the businesses already regulated, and the nature of these firms.

The Department has not quantified the benefits in the NPSV, as it is not possible to estimate the number of avoided attacks associated with the proposal. However, the IA has provided sufficient qualitative explanation of the potential benefits, alongside useful case studies to indicate their scale and standalone estimates of the loss from attacks, where relevant. The IA also conducts break-even analysis to estimate the number of avoided attacks required for firms to 'break-even' and cover their costs.

Appraisal of the shortlisted options

The Department explains the methodology underpinning the monetised estimates, setting out the key assumptions and data sources that have been utilised. Data has been gathered from a variety of sources, including the ONS, internal research and economic modelling conducted by KPMG. The IA also utilises analysis conducted in previous PIRs to form the monetised costs, scaling up these cost-per-firm estimates by the number of regulated entities now in scope. The Department explains that these original unit cost estimates have been calculated using survey responses and ONS data but could provide more detail on the original methodology, including the steps that have been taken to produce these estimates.

Furthermore, the IA could benefit from further explaining some of the assumptions underpinning the cost analysis. For instance, the Department should explain the origin of the assumptions on the number of professions required to familiarise and the number of hours taken to familiarise, justifying why these assumptions are the same for all types of new regulated entities when they may have a different structure of professions. Similarly, the IA could further explain the assumptions underpinning the length of time legal professionals take to change the contracts for the measures (ranging from 8 to 80 hours). The Department could also further explain the methodology underpinning the estimated number of data centres in scope (64). Whilst the IA states that this has been calculated using research commissioned by the Department's data policy team, further detail could be provided on the methodology and representativeness of this research.

To account for uncertainty, the Department has adjusted the number of organisations in scope, creating a low to high range. The IA also increases significant input variables by 20% to form a sensitivity analysis. It is not clear how these adjustments have been derived, and whether the sensitivity analysis is arbitrary +/- percentage adjustments using value judgements. The IA would therefore be improved if the Department were able to include some better-informed sensitivity analysis to test a wider variety of variables.

Selection of the preferred option

The IA explains that implementing the primary legislation package of preferred option reforms is the overarching preferred option. The IA outlines some key reasons for

selecting this as the preferred option compared to the 'do-nothing' option. This set of options will allow the Department to meet the Government's objectives of increasing cyber resilience and future proofing the NIS Regulations in an ever-changing cyber environment, whilst maintaining an environment that is not overburdensome to businesses and essential services. Without updating the NIS Regulations, the UK's national security would continue to be vulnerable to state sponsored threat actors. This provides sufficient qualitative justification.

Regulatory Scorecard

Part A

Impacts on total welfare

Despite a negative NPSV of -£1,201m, the Department considers that the proposal will have a positive impact on total welfare, due to significant non-monetised benefits to society from a reduction in cyber attacks. The Department presents break-even analysis for this benefit elsewhere in the IA but could benefit from including the results from this analysis in the regulatory scorecard to support the description of this impact.

Impacts on business

The Department presents an EANDCB of £137.7m for the preferred option. This EANDCB consists of the costs for businesses to comply with the measures, including one-off familiarisation costs, additional physical security costs, contract change costs and cyber security costs. These costs will be incurred by newly regulated entities, including managed service providers, data centres and large loads controllers. All businesses in scope of the regulation (including those that are currently regulated under the 2018 NIS regulations) will also incur incident reporting costs.

The IA could benefit from setting out the calculations underpinning the EANDCB metric calculation, confirming whether the costs to regulators have been included as a business cost in the calculation. The IA could also provide further clarity on the direct and indirect classification of costs included in the EANDCB calculation, as it is not clear why the costs from Measure 7 (Ensuring that the Information Commissioner's Office (ICO) has the appropriate information related to risk) do not count as direct impacts to business, as they place a duty on relevant digital service providers and relevant MSPs.

The IA states that, despite this negative EANDCB, the preferred option is expected to have a positive impact on business due to the significant non-monetised benefit from the prevention of cyber attacks. The Department explains that the improvement in security would benefit the UK's economic prosperity and output. However, the IA would benefit from detailing non-monetised benefits that relate to businesses rather than society as a whole. In particular, the IA could include a summary of the break-even analysis, that was conducted to show how a reduction in one attack per business exceeded the cost to these businesses for complying with the regulations.

Impacts on households, individuals or consumers

The IA states that households will not be directly impacted by the updated NIS regulations but will experience the indirect benefit from the enhanced prevented of cyber attacks. The IA could benefit from further explaining this impact, perhaps using any relevant case studies from the impact of cyber attacks on individuals, such as NHS patients.

Distributional impacts

The Department states that it does not expect there to be any distributional impacts from the proposal. However, the IA would be improved by further considering any business groups who will be disproportionately impacted by the preferred option, such as particular business sectors or industries. This could include qualitatively detailing the impacts on businesses in the digital sector and electricity sector. The Department could also consider any distributional impacts felt by different household groups. For instance, the spillover effects to individuals from the preferred option may be felt more by individuals more likely to be victims of a cyber attack or those who would face disproportionate costs from an attack. This could include more vulnerable individuals with protected characteristics, or individuals in low-income groups.

Part B

The Department considers the impact of the proposal on wider government priorities, explaining that the policy will support business environment by stabilising the business environment so that businesses can feel confident to grow and innovate without fear of a cyber attack. The IA could be improved by providing any relevant evidence to illustrate the scale of this impact for business, perhaps by utilising any relevant results from industry engagement.

The Department indicates that the policy will also have a positive environmental impact, as requiring cyber security requirements in the load control market will increase consumer confidence in a nascent sector and encourage the adoption of smart, flexible energy solutions.

The IA explains that whilst the regulations may impose costs for some non-UK businesses, as the regulations apply to any entities that provide any regulated service whether established in the UK or not, the preferred option is still expected to have a positive international impact. The proposal will make UK digital firms more appealing to international clients and partners, aligning UK business with global norms on cyber security, helping them export services or attract international investment. The IA could benefit from expanding on this impact, further considering the positive impact from the proposal aligning GB cyber security with EU regulations.

Monitoring and evaluation

The IA provides a satisfactory monitoring and evaluation plan, confirming that it will conduct a post-implementation review within five years of implementation.

The IA explains that the PIR will include carrying out process and impact evaluation. The Department outlines the data sources which will be used to underpin this review, including engagement with regulators, formal surveys, Statement of Strategic Priorities annual reporting and NCSC Cyber Assessment Framework returns data. The IA could benefit from including further detail on the nature of this qualitative and quantitative data and how it will be gathered. This could include identifying the key research questions that will be used in the NCSC data, as well as when the engagement with regulators will take place. The IA should clarify how the survey will be rolled out. While the IA commits to conducting an impact evaluation as part of the PIR, it does not address the fundamental challenge of attribution - whether it will be possible to isolate the effects of these regulatory provisions from other factors affecting cyber security outcomes, and if so, what identification strategy will be employed to establish causality.

The IA identifies existing evidence gaps, such as the number of critical suppliers designated and explains how the proposed monitoring and evaluation will aim to fill these gaps. The Department also explains the limitations with using top down metrics in the review, such as a reduction in cyber incidents, as this may be counterintuitive and not accurately reflect good cyber security or the regulations' performance. Instead, the IA proposes four key performance indicators from regulators, including incidents, capability and improvements. The IA could discuss any possible unintended consequences from the policy, and provide detail on how the evaluation plan will attempt to assess these impacts. The IA could also consider any external factors that will have an impact on the success of the intervention.

The monitoring and evaluation plan also considers how the proposal will impact innovation, trade and competition, stating that the Department will collect information on trade and the concentration of markets. The IA could expand on this, further explaining how this information will be collected.

Regulatory Policy Committee

For further information, please contact enquiries@rpc.gov.uk. Follow us on X @RPC_Gov_UK, LinkedIn or consult our website www.gov.uk/rpc. To keep informed and hear our views on live regulatory issues, subscribe to our blog.