Network and Information Systems Regulations 2018

Lead department	Department for Digital, Culture, Media and Sport
Summary of measure	The Network and Information Systems Regulations 2018 aim to improve the security of network and information systems critical to the provision of essential services and certain digital services which, if disrupted, could cause significant economic and social harm. This is, in line with statutory requirements, the second review of the regulations.
Submission type	Post-implementation review
Implementation date	10 May 2018
Department recommendation	Amend
RPC reference	RPC-DCMS-4456(2)
Opinion type	Formal
Date of issue	31 May 2022

RPC opinion

Rating[1]	**RPC opinion**
Fit for purpose	The PIR presents a proportionate level of evidence and analysis to support the recommendation to make improvements to the regulations that the Department is currently consulting on. The PIR would benefit from providing greater clarity on which findings informed the consultation and where it is making recommendations for future improvements.

[1] The RPC opinion rating is based on whether the evidence in the PIR is sufficiently robust to support the departmental recommendation, as set out in the better regulation framework. The RPC rating will be fit for purpose or not fit for purpose.

RPC summary

Category	Quality[2]	RPC comments
Recommendation	**Green**	The RPC considers the evidence and analysis presented in the PIR to be proportionate and sufficiently robust to support the recommendation to make amendments to the regulations.
Monitoring and implementation	**Satisfactory**	The PIR conducted on-line surveys to gather quantitative and qualitative findings relating to whether the regulations are achieving their objectives and the cost of implementation. For the next PIR in 2027, the Department should aim to improve the response rate of future surveys and the quality of data for the number of cyber incidents reported.
Evaluation	**Satisfactory**	The PIR presents survey findings to show that some of the key objectives are being met. Areas for improvement are evidenced from the findings, which the Department are considering as part of amending the regulations. The surveys indicate that the costs to business are higher than anticipated in the original impact assessment. Therefore, the Department should consider conducting a more rigorous evaluation to inform the 2027 PIR.

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

Summary of proposal

The objective of the Network and Information Systems Regulations, which came into force on 10th May 2018, is to improve the security of network and information systems critical to the provision of essential services and certain digital services. If these services are disrupted, for example, by cyber-attacks, it could cause significant economic and social harm.

The Regulations apply to operators of essential services in the transport, energy, water, health, and digital infrastructure sectors, and to relevant digital service providers (cloud computing services, online marketplaces, and online search engines).

For operators of essential service or relevant digital service providers that fall within the designation thresholds, the Regulations specify that they must:

- take appropriate and proportionate measures to ensure the security of the network and information systems used to provide their essential services, both by managing risk and by minimising impact of any disruption; and
- notify their Competent Authority about any incident which has an adverse effect on the security of the network and information systems used to provide their essential services, according to criteria set out in incident reporting thresholds.

Recommendation

The post-implementation review (PIR) recommends amending the NIS Regulations. The Department has presented a proportionate and sufficient evidence base in this second review of the regulations to demonstrate that key objectives are being met since implementation in 2018. The early findings of the PIR relating to areas of improvement were used to inform a recent consultation on legislative changes to the regulations. The PIR would benefit from a clearer presentation of its findings and how these support the recommendation and the identified improvements currently being consulted upon.

Monitoring and implementation

Proportionate

The Department has followed a similar ‘medium’ resource approach to this PIR to that used in the first review conducted in 2020 and assessed as fit for purpose by the RPC in its opinion of 14 April 2020. The monitoring and evaluation activities are proportionate for the scale of business impacts estimated in the original impact assessment accompanying the introduction of the NIS regulations. However, in light of the upward revision to the EANDCB reported in the latest PIR (discussed below), the Department may wish to plan for a more rigorous evaluation as part of the next review in 2027.

Range of evidence
The PIR describes the sources of data and evidence that have been used to inform the findings and recommendations. Four separate on-line surveys were conducted with the key groups of stakeholders: operators of essential services; relevant digital service providers; competent authorities; and the National Cyber Security Centre (NCSC).

Since the regulations had only been in force for three years at the time the surveys were issued, the questions focus on organisations' experiences of the regulations and their implementation rather than impact. Building on the lessons of the first PIR, the Department included additional qualitative questions into the surveys to gain more understanding organisations' quantitative responses to inform future policy development.

Although the surveys achieved responses from a range of sectors and both medium and large organisations (no smaller organisations were identified as being in scope), the response rates were lower compared to the previous 2020 PIR. Only 16 per cent of operators of essential services and 8 per cent of digital service providers responded, compared to an overall 23 per cent response rate across both groups in 2020. The Department explains that the poor response rate may be attributable to the impacts of Covid-19 or a reduced willingness to participate in a second round of surveys. For the next PIR in 2027, where the focus of the M&E activities would be expected to shift from implementation to evaluation of impact, the Department should develop a range of approaches to maximise the response rate for future surveys if they are to inform an understanding of the long-term effectiveness of the regulations.

Gaps in evidence justified
The PIR acknowledges that the lack of an established counterfactual for the number of incidents creates difficulty in assessing whether the regulations have had an impact on reducing the number of incidents. While the number of NIS incidents decreased from 13 in 2019 to 12 in 2020 there also remains uncertainty regarding whether the current reporting requirements are accurately capturing incidents, both in terms of volume and the potential severity of impact on the economy. Reporting of NIS incidents should be improved as soon as possible to enable a robust evaluation and PIR to be undertaken in 2027.

Evaluation

Policy objectives considered
As noted above, data limitations prevent the PIR from estimating the impact of the regulations on the number of incidents. However, the survey results provide supporting evidence in the first three years of implementation against the policy objectives to "prevent and improve the level of protection against network information and security incidents" and "ensure that there is a culture of security across sectors which are vital for our economy and society" (page 23). For example, the survey of operators of essential services found that 28 per cent and 51 per cent had either introduced, or updated, policies or processes since the regulations were

implemented and 71 per cent reported an increase in board support for cyber security.

When presenting the survey results, the PIR would be improved from greater clarity on whether the changes to policies and processes reported by organisations are considered attributable to the NIS regulations. Competent Authorities reported that the regulations are likely to have accelerated improvements to cyber security rather than generated new improvements. The surveys also reveal that prior to implementation of the regulations, changes to the security of network and information systems were already being implemented in response to other regulations (e.g. UK General Data Protection Regulations) as well as non-regulatory reasons (e.g. avoiding financial loss or reputational damage).

Unintended effects
The PIR notes that there is little evidence to suggest there have been any unintended consequences from implementation of the NIS regulations. For the next PIR in 2027, the Department could explore if good practice in managing cyber risks in the essential services and digital services resulting from the regulations has been adopted by other businesses in non-regulated sectors.

Original assumptions
The RPC commends the Department for presenting a detailed analysis of how the actual costs of the regulations compare to those presented in the original impact assessment. Table 2 shows that familiarisation costs, compliance costs and security costs are all higher than originally estimated due to the inclusion of self-reported data on costs incurred from the PIR surveys and updated assumptions of the numbers of staff involved and their wage rates. However, the cost of reporting incidents is found to be significantly lower as only 13 incidents were reported per year compared to an assumption of 1,348 in the IA. Overall the EANDCB is now estimated to be £49.2m compared to £20.4m at the time of the IA (both in 2014 prices and 2018 present value base). With changes to the reporting arrangements and thresholds for the number of NIS incidents and their severity, there would appear to be scope for the EANDCB to increase further. The Department could seek to consider this within the next PIR.

Intervention required and improvements
The recommendation to amend the regulations is supported by the findings of the PIR in relation to security improvements in network and information systems occurring at an accelerated rate than would otherwise be the case. Without the regulations, there would be a risk to emerging sectors, customers and the wider economy if operators provide insecure services. The Department considers alternative approaches such as raising awareness of cyber security but argue that they are likely to be most applicable to businesses that would be of low risk to the economy in the event of security breach.

The Department has already made some amendments to the regulations based on the first PIR conducted in 2020 and has recently consulted on further changes which have partly been informed by the early findings of the latest 2022 PIR. Some of the key areas for further change which have been informed by the PIR's surveys include:

- **registration of relevant digital service providers** – 54 per cent of providers reported difficulties in understanding if they were required to register with the Information Commissioners Office, creating challenges for implementation of the regulations;
- **ensuring the right organisations are in scope** – some competent authorities continue to report that not all of the correct organisations are being designated and the scope should be expanded;
- **supply chain risks** – 9 per cent of operators of essential services have the resources to manage the risks from their supply chains;
- **capability and capacity constraints** – competent authorities, operators of essential services and relevant digital service providers all reported skills constraints among staff when implementing the regulations

The PIR would be improved by providing greater clarity of the specific details and timings of the changes that have already been made to NIS Regulations, those currently being consulted on, and any remaining proposals for future amendments which have been directly informed by the findings of the latest 2022 PIR.

Regulatory Policy Committee

For further information, please contact regulatoryenquiries@rpc.gov.uk. Follow us on Twitter @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.