Title: Cyber Security Measures
IA No:

RPC Reference No:

Lead department or agency: Department for Digital, Culture, Media, and Sport. (DCMS)

Other departments or agencies:

Impact Assessment (IA)

Date: 01/10/2021

Stage: Consultation

Source of intervention: Domestic

Type of measure: Primary Legislation

Contact for enquiries: Network and Information System Team
NIS@DCMS.Gov.UK

Summary: Intervention and Options

RPC Opinion:

Cost of Preferred (or more likely) Option (in 2021 prices)			
Total Net Present Social Value	**Business Net Present Value**	**Net cost to business per year**	**Business Impact Target Status**
£1,415.9m	£1,415.9m	£141.6m	

What is the problem under consideration? Why is government action or intervention necessary?

Cyber threats to national security, critical infrastructure, and essential services are on the rise; threats not present only a few years ago can cost the UK economy billions today and put the societal and economic well being of the country at risk. The cost of cyber attacks was estimated to be up to £27bn per annum in the UK[1] These large costs faced by the UK economy are not mirrored by the costs faced by the firms that are attacked, creating large negative externalities.

It is vital that the government intervenes to ensure that the regulatory frameworks aimed at protecting these interests are effective, updated, and can deliver on the UK's objectives of being an international cyber power.

The proposals aim to solve a number of issues relating to supply chain vulnerabilities, lack of reported cyber incidents, and lack of updating provisions within the already-established Network and Information Systems Regulations 2018. (NIS)

What are the policy objectives of the action or intervention and the intended effects?

To improve the cyber resilience of organisations that have a large impact on the UK economy. This means improving both the cyber security of these key firms and their ability to respond to cyber incidents. These will be measured in the post-implementation reviews of the NIS Regulations. These benefits of the policy should begin swiftly after the regulations are implemented and should be captured in the next NIS Post-Implementation Review, which is due to be published in 2027. DCMS also aims for this policy to be a relatively low cost to business, so the reviews will capture whether the costs have been as forecasted.

What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base)

The 2020 Post-Implementation Review of the 2018 NIS Regulations found that the regulations were not fit for purpose in several ways. It recommended a number of changes to the regulations. This package of measures looks to update the measures to ensure that market failures that exist are addressed, and to reduce the time it takes to act on future market failures.

The amendments to the existing regulations explored in this IA are:

- Changes to the supervisory regime of Data service Providers;
- Expanding the definition of data service providers;
- Allowing the minister to amend the existing regulations;
- Allowing the minister to designate sectors and sub-sectors as part of the regulations;
- Allowing the minister to designate critical dependencies as part of the regulation;
- Amending the incident reporting duties covered by the regulation;
- Giving competent authorities the power to recover the costs of the regulations.

Where appropriate, the option to produce guidance has been explored as well as several options for implementation of these measures. As the benefit to individual businesses of implementing these measures will tend to be less than the cost, businesses do not have an incentive to implement these measures, guidance is ineffective and would allow the negative externality. The preferred option for all these measures is to enact regulation for reasons set out in the evidence base of this document.

Is this measure likely to impact on international trade and investment?		No		
Are any of these organisations in scope?	**Micro: Yes**	**Small: Yes**	**Medium: Yes**	**Large: Yes**
What is the CO_2 equivalent change in greenhouse gas emissions? (Million tonnes CO_2 equivalent)		**Traded: N/A**	**Non-traded: N/A**	

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

Will the policy be reviewed? It will be reviewed. **If applicable, set review date:** 05 /2027

I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.

Signed by the responsible : Catherine Colebrook Date: 01/10/2021

Summary: Analysis & Evidence

Policy Option 1

Description:

FULL ECONOMIC ASSESSMENT

Price Base Year	PV Base Year	Time Period Years	Net Benefit (Present Value (PV)) (£m)		
2021/22	2021/22	10 years	**Low: -£937.1m**	**High: -£1,896.3m**	**Best Estimate: -£1,416.7m**

COSTS (£m)	Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	Optional		£116.2m	**£936.9m**
High	Optional		£234.9m	**£1,894.9m**
Best Estimate	£1.2m		£175.1m	**£1,415.9m**

Description and scale of key monetised costs by 'main affected groups'

The main affected groups of this are the firms that are currently regulated by the NIS Regulations and the firms, such as managed service providers, that some of the measures look to include in the NIS Regulations. These firms will face the costs of familiarising themselves with the legislation, the costs of improving their cyber security, the costs of reporting incidents and complying with the regulations as well as the costs of the competent authorities applying the regulations.

Other key non-monetised costs by 'main affected groups'

Most of the known costs have been monetised or included as a demonstrative cost. Some other costs, like the costs to some of the competent authorities (CAs) as a result of the measures have not been monetised as the impact of the policies are not yet known. Through consultation and regular meetings, DCMS aims to close these gaps.

BENEFITS (£m)	Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	Optional		Optional	**Optional**
High	Optional		Optional	**Optional**
Best Estimate				

Description and scale of key monetised benefits by 'main affected groups'

NA

Other key non-monetised benefits by 'main affected groups'

The firms will likely have a reduction in the amount of cyber breaches that result in a loss or reduce the loss as a result of a breach, this cannot be monetised as the benefits of the previous legislation had not yet materialised by the time of the last review. The external benefit of regulating these firms is the reduction in loss faced by the wider economy as a result of a loss of service faced by these cyber breaches. Other reported benefits of these regulations has been an increase in cyber security being discussed at the board level.

Key assumptions/sensitivities/risks	Discount rate (%)	3.5 %

Some of the measures included in this IA are very uncertain in what their impact might be. DCMS will work with regulators and the sectors themselves to close these key gaps before the final IA.

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m:			**Score for Business Impact Target (qualifying provisions only) £m:**
Costs: **£141.6m**	**Benefits: N/A**	**Net:** **-£141.6M**	

Evidence Base

Problem under consideration and rationale for intervention

This IA covers 7 different regulatory changes to the NIS Regulations. These 7 measures aim to reduce negative externalities produced by under investment by firms in their cyber security. This negative externality is created as the costs of a successful cyber breach to the wider UK economy is larger than that to the business itself. The NIS Regulations are targeting the organisations that are essential to the UK economy and have the largest economic consequences of a successful breach.

The 7 measures covered by this IA are titled:

- The supervisory regime for digital service providers;
- Expanding the definition of digital service providers;
- Measures to allow a Minister of the Crown to make secondary legislation to update the regulations in the future;
- Measures to allow a Minister of the Crown to make amendments to the scope of NIS sectors and sub-sectors;
- Measures to allow a Minister of the Crown to designate critical dependencies that are fundamental to the provision of the essential service;
- Measures to amend the incident report duties of organisations in scope beyond the limit of continuity of service; and
- Measures to allow NIS competent authorities to recover the full costs of regulatory activities.

This document will address the rationale, options, objectives and costs of each measure in-turn and to make a clear case for each measure. Where there are interactions between 2 measures this has been pointed out.

The supervisory regime for digital service providers

Digital service providers are key enablers of the digital transformation of the UK's economy. They provide digital services that are essential to the operational continuity and resilience of organisations across the economy, including the UK Government and critical national infrastructure**.** For instance, the Parliamentary Office of Science and Technology in June 2020 put forward estimates that 89% of larger UK organisations use at least one cloud-based service.[2]

[2] https://post.parliament.uk/research-briefings/post-pn-0629/

Yet, recent cyber incidents such as Operation Cloud Hopper[3], SolarWinds[4] and Kaseya[5] demonstrate that cyber threats are increasingly reaching organisations through vulnerabilities in their supply chains via digital service providers. This is reinforced by the *Cyber Security Breaches Survey 2021,* which found that only 12% of businesses review risks coming from immediate suppliers while only one in twenty address risks coming from wider supply chains.[6] Similarly, the 2020 NIS Post-Implementation Review[7] highlighted the need for the NIS Regulations to better address supply chain risks. By failing to address the supply chain cyber risks associated with digital service providers, the NIS Regulations are failing to achieve their aims as envisaged.

Given the ubiquity of digital services throughout the economy and the number of users, effective regulation of digital service providers will be instrumental to securing supply chains across all sectors, whether within the scope of NIS or otherwise. When digital service providers are supplying essential services at scale, their vulnerabilities present a systemic threat to the UK's national security and economic prosperity. This large cost to the wider economy of a successful cyber attack presents a negative externality, where the costs of poor cyber security to the firm are smaller than those faced by the wider economy. The government needs to step in to address the underspending on cyber security and ensure that these systems are secure.

When the original NIS Directive was developed, it also did not foresee the rapid digitisation of recent years. As such, a more light-touch approach was set out to the regulation of digital service providers, which does not reflect the criticality of digital services and their providers today. Yet the Government also recognises that with a large number of digital service providers operating multiple services within the UK economy, from a practical perspective, it is necessary to focus resources on the services that are most critical to the UK's resilience while limiting the regulatory burden, where possible, on those that do not carry systemic dependencies of such magnitude.

The Government therefore proposes to codify the two-tier supervisory regime for relevant digital service providers under NIS. This will involve a proactive supervisory regime for the most critical digital services and a reactive supervisory regime for the remaining digital services regulated under NIS. Digital service providers regulated on a more proactive basis will be required to demonstrate to the Information Commissioner's Office, on an ongoing basis, that they have fulfilled their duties under NIS, Providers under a reactive regime would have the same duties, but only be subjected to lighter-touch supervision. To implement this, the government is proposing the development of criteria to identify the most critical providers of digital services.

---

[3] https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf

[4] https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T

[5] https://www.bbc.co.uk/news/world-us-canada-57703836

[6] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021

[7] https://www.gov.uk/government/publications/review-of-the-network-and-information-systems-regulations

Expanding the definition of digital service providers

The scope of providers of digital services under NIS is currently limited to entities providing online search engines, online marketplaces or cloud computing services. There are a number of other entities that provide digital services to organisations that are vital to the UK's economy and society. These digital services are critical to the functioning, reliability and availability of essential services. The scope of the NIS framework no longer reflects all digitised sectors providing essential services to the economy and society as a whole.

Recent cyber incidents have demonstrated that managed service providers[8] are key providers of digital services that expose significant systemic risks to the UK's economy and critical national infrastructure. Managed service providers often have privileged access to their customer's critical data, IT infrastructure, IT networks and/or IT systems. This makes them attractive targets in and of themselves as well as potential attack vectors or staging points that can be used by threat actors to compromise clients at scale.

The National Cyber Security Centre's experience of working with managed service providers has highlighted that cyber security levels vary widely across the industry. A lack of common cyber security standards has led to the successful exploitation of vulnerabilities including in UK companies, such as those that allow access to thousands of clients in one successful cyber attack[9]. In 2017 several managed service providers were compromised by cyber attacks. This wave of attacks included the Wannacry attack on the NHS. Since then, cyber attacks have evolved and become more frequent[10], and the risk of attackers exploiting vulnerabilities through Managed Services remains high, especially given the impact of the COVID-19 pandemic on the UK's digital transformation. The National Cyber Security Centre assesses that it is highly likely that the rise in incidents involving managed service providers is a result of both the increasing sophistication of the threat actors involved and a growing realisation of the advantages of targeting these providers.

Although there is guidance available to companies through schemes such as National Cyber Security Centre's Cyber Essentials, there is currently no minimum cyber security baseline for managed service providers operating in the UK and very few mandatory cyber security requirements for companies entering this industry. This has resulted in varied levels of cyber security across the managed services industry in the UK and makes it difficult for the Government to gain assurance of the level of cyber resilience in the managed service provider market. As a result, managed service providers can represent a systemic risk to the UK economy and society due to the scale and concentration of services offered by the most critical managed service providers, especially those providing services to critical national infrastructure sectors.

---

[8] A managed service for the purposes of this document has been defined as a service which involves regular and ongoing service management of data, IT infrastructure, IT networks and/or IT systems, is categorised as business to business (B2B) and relies on network and information systems as a service supplied by an external, third party supplier, which involves regular and ongoing service management of IT data, infrastructure, networks and/or system. It is a business-to-business solution.

[9] NCSC Assessment - The Cyber Threat To UK Business https://www.ncsc.gov.uk/files/ncsc_nca_report.pdf

[10] 32% of businesses faced a weekly cyber threat in 2020 vs 22% in 2017. Cyber breaches survey: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020

Including managed service providers under NIS will provide a greater level of assurance over the level of cyber resilience of these critical providers of essential digital services. Evidence from the 2020 NIS Post-Implementation Review[11] indicates that many operators of essential services were putting in place measures which we would expect to lead to improved security outcomes as intended by the original NIS regulations.

As a successful cyber attack on one of these could affect thousands of firms, the risk created by a managed service provider's poor cyber security is much greater than the cost to their own company. This negative externality is the reason the government needs to intervene in the market and ensure that firms' systems are secure enough and that the smaller private cost of a successful breach isn't a barrier to more private investment in cyber security.

Measures to allow the Government to make secondary legislation to update the regulations in the future (amending the legislation for existing business population)

Cyber security threats to UK critical national infrastructure, UK essential services, and even the wider economy and society are on the rise. As technology advances, so does the nature and level of sophistication of cyber threats. The NIS Regulations, as one of the most significant regulatory frameworks in the UK designed to reduce and mitigate these threats, must be able to keep pace with technological change and with advancing sophistication of attacks.

Since 2018, when the regulations came into force, the Government conducted a comprehensive Post-Implementation Review (May 2020, two years after implementation)[12], which concluded that while the regulations were having a positive impact, there already were necessary improvements to be made in order to ensure that the framework delivers on its objectives. This has been achieved via the European Communities Act 1972, Section 2(2), in November 2020. As of EU Exit, the European Communities Act 1972 is repealed and therefore, there is no longer a way to make delegated legislation to update the framework in the future.

This measure seeks to implement provisions to allow the government to make further updating amendments to the NIS Regulations, as required from time to time. This will give the government the ability to respond to the emerging threat and keep pace with technology, and will help guard against the regulations becoming less effective over time.

Any future changes would require secondary legislation, meaning there would still be consultation on the changes, however the process for this would be much shorter than going through primary legislation. With cyber being a rapidly-developing area for policy, it is important that the government can react quickly and effectively to combat threats to network and information systems and reduce the cyber threats created by individual organisations to the wider economy.

---

[11] https://www.gov.uk/government/publications/review-of-the-network-and-information-systems-regulations

[12] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/960574/CCS207_CCS0320329850-001_Network_and_Information_Systems_Regulations_Post-Implementation_Review_Web_V2.pdf

Measures to allow the government to make amendments to the scope of NIS sectors and sub-sectors (expanding the business population covered by the regulations)

Under the current form of the NIS Regulations, currently it is impossible to expand the NIS framework to new sectors beyond the limited amount set by the original EU Directive. To ensure effective regulation, the government needs to make sure it can adapt to the changing landscape of cyber threats to the economy's essential services. Since the creation of the NIS EU Directive in 2018, the understanding of which sectors that are essential to the UK economy are under threat has changed. A lack of regulatory oversight to ensure that these sectors are maintaining adequate cyber security protection leaves the UK open to increased cyber security risks.

This measure differs from the measure to allow the government to make secondary legislation to update the regulations, as the previous measure will only allow for updates to the regulations for the existing business population. The measure to designate sectors and sub-sectors is the power to expand the NIS Regulations rather than to amend them to respond to new requirements or threats.

Allowing the government to make amendments to the scope of the NIS sectors and sub-sectors would solve this issue by granting the government powers to expand the scope of the NIS framework in the future through secondary legislation, to cover additional sectors (e.g. pharmaceutical, postal services, wastewater management, etc.), based on future assessments of risks and impacts of regulations and whilst adhering to under clear and explicit limitations. However, the process for designating a new sector would be much shorter than going through primary legislation, allowing the government to react to new threats and negative externalities swiftly. If this measure is not acted upon, there will be a delay between a systemic threat being identified and those firms being covered by the NIS Regulations and fixing the under investment in cyber security.

For these firms to breakeven from the NIS Regulations the number of successful breaches per firm would have to be very high, to avoid the personal loss by improving their cyber security. The loss to the economy of these firms not acting and improving their cyber security is much greater than the firms themselves. This is why the government needs to act by making these changes to the regulations, to reduce the negative externality created.

Measures to allow the government to designate critical dependencies that are fundamental to the provision of the essential services

Existing NIS regulations require operators of essential services to ensure the provision of services are robustly protected from the threat of cyber attacks by protecting their network and information systems. However, some operators of essential service are dependent on suppliers of products or services that are critical to the provision of essential services, and if these critical dependencies were subject to a cyber attack that inhibited their ability to provide such services or products then the resilience of the entire sector could be threatened.

The complexity and interconnectivity of today's digital environment means that organisations have a limited understanding of vulnerabilities and interdependencies that they and their supply chains are subject to. High profile cyber incidents such as SolarWinds demonstrate how hostile actors are increasingly using vulnerabilities in organisations supply chains to attack their ultimate targets.

Competent authorities, the regulators[13] that implement the regulations, require operators of essential services to secure their supply chains, primarily through contract and procurement measures , for example the Cyber Assessment Framework principle A4 for supply chains. [14] However, there are some entities within individual sectors that are so critical to the provision of an essential service, that relying on contractual agreements to enforce security is inadequate.

This measure addresses the gap by enabling competent authorities to designate critical sector sector dependencies, expanding the remit of the NIS Regulations. This is important as the NIS Regulations currently only apply to those entities that are providing an essential service (such as the provision of water or electricity). Some sectors are dependent on suppliers of products or services that are critical to essential services across the whole sector and without whom the essential service would not be able to operate. As an attack on these critical dependencies could cause the same level of damage as an attack on the current firms regulated by NIS Regulations, the same negative externality of the impact of a cyber attack still exists in these firms. It is therefore important to regulate these firms so they are mandated to improve their cyber security to the levels required by the NIS Regulations. This will help to address the large social cost of a cyber attack, which far outweighs the negative private cost of an attack.

Measures to amend the incident report duties of organisations in scope beyond the limit of continuity of service

This measure proposes to broaden reporting requirements for incidents under NIS to include incidents that do not affect continuity of service but that have the potential to impact the service.

One of the key duties of organisations in scope of the NIS Regulations is the duty to report incidents under regulation 11. This allows the competent authorities, in their role as regulators, to intervene, provide support and guidance, and involve the necessary national authorities (either the National Cyber Security Centre for their technical expertise or law enforcement, etc. in case of criminal activities, as well as other entities).

A fundamental qualifier of what incidents must be reported in the NIS Regulations is the fact that such an incident must affect continuity of service (i.e. the incident in question must have damaged / created a scenario in such a manner that the essential service, such as drinking water or energy distribution, would cease to function).

---

[13] The UK's competent authorities are: the Secretaries of State for Business, Energy, and Industrial Strategy; Environment, Food, and Rural Affairs; Transport; Health and Social Care; Scottish Ministers; Welsh Ministers; Department of Finance, Northern Ireland; Ofgem (jointly with BEIS); Ofcom; Civil Aviation Authority; Drinking Water Quality Regulator for Scotland; and the Information Commissioner's Office.

[14] https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/a-4-supply-chain

Organisations in scope can choose not to report incidents that have a high risk of taking the service down in the near future, (i.e. ransomware or other types of malware installed on essential systems), as long as they have not disrupted the service.

By changing the reporting requirements to include incidents with the *potential* to disrupt the service, regulatory authorities will be able to respond to a wider range of incidents (e.g. ransomware precursor malware) and will be able to provide support before the essential service is impacted and loss of service occurs.

Currently, there have been very few cyber security incidents reported under the NIS Regulations; while it is possible to lower the thresholds (e.g. the numerical criteria setting out at what level of impact an incident is legally reportable) via statutory guidance, the regulations do not allow the government to require cyber security incidents that do not affect continuity (as an example, ransomware attacks that encrypt personal files and hold the company to ransom but do not affect critical systems) to be reported.

Several incidents in recent memory serve to prove how incidents may have a very detrimental effect on organisations in scope, even though service was not affected, and these vulnerabilities may be exploited by other actors with much more devious intent. The recent Northern Rail attack for instance, where the transport's ticket machine supplier (Flowbird) was hit by a ransomware attack[15], was not reportable under NIS - but made headlines everywhere. Thus the competent authority had no means of determining whether this incident could leak over from the ticket machines to critical systems, and eventually halt train services.

Such incidents have a very high possibility of affecting continuity of the service in the future. It is vital that the regulations can require operators to disclose such important events, so that the regulators have an accurate, up-to-date understanding of the threat landscape, and can consequently request that the entities take appropriate action to mitigate those risks. Such action could stop large losses by these organisations and allow the government to fully understand and therefore advise organisations how to respond to threats and breaches.

Measures to allow NIS competent authorities to recover the full costs of regulatory activities

This measure proposes two changes. Firstly, to shift the total costs of NIS implementation onto industry; secondly, to change the way in which regulators recover their costs from regulated entities.

Competent authorities cannot currently charge industry for enforcement activities (penalties and their enforcement, appeals, civil proceedings, and the enforcement of penalty notices). This means that the regulation of these firms is currently being directly subsidised by the government. This creates an inefficient allocation of resources as the taxpayer is subsidising the regulation of entities. Treasury guidelines for managing public money outlines the approach that should be taken, 'certain public goods and services are financed by charges rather than from

[15]"Northern Rail reports cyber attack on self-service ticket machines", Railway Technology, 20 July 2021 https://www.railway-technology.com/news/northern-rail-cyber-attack/

general taxation.The standard principle is to set charges to recover full costs, an approach that is intended to ensure government and public bodies neither profit at the expense of consumers nor make a loss for taxpayers to subsidise'.[16]

Having full cost recovery powers would also translate into better implementation of the NIS Regulations; for instance, operators of essential services and relevant digital service providers may rely on some of the provisions in the regulations (such as appealing an Enforcement Notice simply to delay the process or frustrate the penalty regime in order to gain more time) because it bears no cost to the operators themselves and have more to gain from delaying implementation.

This reliance on public funds is highly inappropriate for the rapidly-evolving nature of the sector that NIS competent authorities regulate, and leads to financial obstacles. They do not have the flexibility, once a centrally-funded budget has been approved, to react to unpredictable increases in their workload until the next government funding bidding round.

By expanding NIS' cost recovery powers to include enforcement activities, the measure seeks to ensure that competent authorities are able to transfer the full cost of compliance onto the organisations in scope, rather than rely on the taxpayer to front the costs (i.e. through funding from Her Majesty's Treasury (HMT)).

In addition, this measure seeks to change how regulators recover costs for their regulatory activities from industry. The current mechanism under NIS has certain limitations. It is recovery-based, meaning that regulators mainly collect recoverable costs in arrears. For some competent authorities, this means that they have to finance their costs for recoverable activities from sources other than industry (i.e. from public funds) in the interim, until these costs can be recovered historically from industry through invoicing (which can be up to a year after the expenditure for recoverable costs was incurred). As a consequence, some competent authorities rely on public funds to finance NIS costs in the interim, which is contrary to the overall objective of removing the cost burden from the taxpayer.

This measure therefore proposes to reevaluate the cost recovery mechanism. By removing the wording within NIS regulations that limits competent authorities to recovering historic costs, regulators would have the freedom to design their own cost recovery system or make it more consistent with existing ones used for their other regulatory duties. This could lead for example to hybrid cost recovery models, where competent authorities could both implement a fees system (i.e. annual, quarterly or monthly fees are collected from industry in advance) and have direct cost recovery powers to the firms that incur the costs.

Rationale and evidence to justify the level of analysis used in the IA (proportionality approach)

This impact assessment has used the previous Post-Implementation Review of the NIS Regulations to identify the issues with the current NIS Regulations. This provided the first step in identifying the rationale for intervention.

[16] See Principle 6 of the Managing Public Money Guidelines by HM Treasury, available here.

Where possible, data from the Network and Information Systems Post-Implementation Review has been used to identify the best policy proposals and assess the impacts on the policy.

Any gaps in the evidence base have been clearly highlighted, and DCMS will attempt to improve the evidence base for the final stage IA. Where possible, DCMS has engaged industry to understand how the legislation could impact society. This engagement includes: regular meetings with competent authorities to understand how some of the measures could work in practice; meetings with the expert advisory group to test some of the policy thinking and assumptions with firms; and meetings across other government departments to gain the views of experts in different sectors. This engagement has allowed DCMS's knowledge of the impact of each measure to be tested prior to consultation. More engagement will continue, and the post-implementation review due to be published in 2022 will supply additional evidence.

Some of the gaps highlighted by the preliminary analysis have been identified as questions for the consultation. One of the main gaps in the appraisal of the measures described in this document is the impact of reporting measures that do not affect continuity of service. As DCMS has a limited understanding of how firms triage cyber incidents, an estimate has not been possible on the increase in incident reporting. The consultation should allow a full appraisal of this measure by the final Impact Assessment.

Description of options considered

The supervisory regime for digital service providers

Option 1: Do nothing

To do nothing would not address the market failure described above and therefore is not a viable option.

Option 2: Codify the two-tier supervisory regimes which will involve a proactive (ex-ante) supervisory regime for the most critical digital services and a reactive (ex-post) supervisory regime for the remaining digital services regulated under NIS.

This would address the market failure by ensuring that data service providers that present the greatest risk to the economy through their impact will have their security proactively monitored.

Option 2 is the preferred option of this measure.

Expanding the definition of digital service providers

Option 1: Do nothing

This would not address the market failure present, as this has not been corrected without government intervention.

Option 2: Designate all managed services provided by large and medium providers as within the scope of the NIS Regulations. Small and micro businesses would be exempt, unless designated by the competent authority as critical.[17]

This intervention would address the market failure mentioned above. The intervention would ensure that all these firms reported on any incidents and allowed competent authorities to intervene where necessary, including in small and micro organisations which provide the most critical services.

Option 3: Designate all managed services as part of the NIS Regulations.

The firms with the largest externalities from their cyber risk are the medium and large firms covered by the regulations, as these are the firms with the largest number of customers. To regulate all services provided by small and micro managed service providers that exist in the economy could place an unfair burden on these small and micro businesses and not address a large negative externality that exists in the larger firms. DCMS is therefore planning to continue the exemption by default to small and micro businesses which applies to digital service providers, with the exception of those deemed critical by the relevant competent authority. DCMS, therefore, proposes not to carry option 3 forward.

[17] DCMS recognises that any relaxation of the small and micro firm exemption must be proportionate to risk. Evidence is therefore being gathered through the public consultation process on the impact of relaxing this exemption, this will be reflected in the final impact assessment.

Option 2 is the preferred option of this measure.

Measures to allow the government to make secondary legislation to update the regulations in the future

Option 1: Do nothing

This is a viable option but could leave the UK economy exposed to the changing risks posed by cyber. This option could allow the market failure of underinvesting in cyber security

Option 2: Give the government updating powers to make amendments to the NIS Regulations, via secondary legislation, to ensure they remain effective. These powers will be subject to certain restrictions, ensuring that any amendments do not expand the scope of the regulations.

Option 2 is the preferred option of this measure.

Measures to allow the government to make amendments to the scope of NIS sectors and sub-sectors

Option 1: Do nothing

Doing nothing, to date, has meant the issues described above have not been addressed. The market has not effectively increased the cyber security of other essential services enough to reduce the threat it poses to the economy as can be seen in the case of managed service providers. Whilst these sectors are often governed by the General Data Protection Regulations (GDPR), this has only increased the security around personal data and not for the systems that relate to the operation of the essential services.

The European Union, which was the source of the original legislation, has also identified that more sectors need to be covered by the regulations. In the implementation of NIS 2.0, the EU has extended the sectors under the NIS regulations to include 8 additional sectors.[18] This shows that internationally, countries are recognising the growing threat to other sectors.

Option 2: Through guidance, and other non-legislative means, encourage better cyber practices in target sectors

This option, which has been effectively the approach taken so far, has proven to be ineffective. As was highlighted in the initial NIS consultation, businesses often do not have a comprehensive understanding of the costs or benefits of cyber security to their business. As a result, investment in cyber security and resilience is often deprioritised.

This has not changed since the implementation of NIS back in 2018. Recent reports highlight the continuing level of cyber resilience of businesses operating across the UK. Only half of businesses (46%) have a dedicated budget for delivering their cyber security strategy[19]. The

[18] https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2
[19] FTSE 350 Cyber Governance Health Check

increased risk level noted under Covid-19 with fewer businesses deploying security monitoring tools (35%, vs. 40% last year) or undertaking any form of user monitoring (32% vs. 38%)[20], only highlights the necessity for government intervention.

Guidance is also sector-agnostic and does not provide advice for specific threats for a certain sector; the NIS Regulations apply to designated sectors and competent authorities work collaboratively with regulated entities to assess their security of network and information systems, their vulnerabilities, and provide specific advice to manage and mitigate those risks. As the condition for inclusion in NIS is that a sector provides an essential service to the UK economy and society, the balance between independent security and the risks arising from poor risk management practices is uneven. If a sector would be deemed to be important enough to merit inclusion in the NIS Regulations then generic guidance without active supervision and tailored advice is not sufficient.

Due to the high cost of implementing some of the cyber security improvements, firms are unlikely to act on guidance alone, even if it was sector specific. Therefore a non-regulatory approach is not viable if we truly are committed to protecting British consumers from the disruption of their essential services.

Option 3: Grant the government the power to designate new sectors under the NIS Regulations

This option best addresses the weaknesses of the current regulations, and ensures that the government can react quickly to address any market failures. This option enables more flexibility than the EU's changes to the NIS Regulations, as primary legislation will not be required to implement the changes.

Option 3 is the preferred option of this measure.

Measures to allow the government to designate critical dependencies that are fundamental to the provision of the essential services

Option 1: Do nothing

This would allow key organisations to go unregulated and still allow the possibility of a large negative externality created by poor cyber security to go unregulated. The NIS Post-Implementation Review highlighted that supply chains were a current limitation of the NIS Regulations. Doing nothing would allow that limitation to exist and possibly harm the effectiveness of the regulations.

Option 2: Voluntary advice and guidance

The existing Cyber Assessment Framework requires relevant firms regulated under NIS to secure their supply chains through contractual means. The government, working through the competent authorities, could issue further advice and guidance, or make amendments to the existing Cyber Assessment Framework, to raise awareness of the threat arising from 'critical

[20] *Ibid.*

dependencies'. This would be supported by guidance on how to voluntarily work with the competent authorities to identify and manage these dependencies.

The effectiveness of advice and guidance is limited for the following reasons:

- 'Critical dependencies', by their nature as the sole supplier to many firms involved in the provision of essential services in highly concentrated markets, exhibit strong market power. This structural imbalance means that the firms directly involved in the provision of essential services ability to require 'critical dependencies' to improve their cyber security through contractual means is severely curtailed. Addressing this market failure calls for sector wide regulatory intervention (Option 3).
- Guidance does not place reporting duties on OESs to require specific information from 'critical dependencies' necessary to manage risk, nor does it provide the necessary enforcement measures to compel 'critical dependencies' to improve their cyber security management.

Given the scale of the threat posed to essential services by hostile attackers seeking to use vulnerabilities in their supply chain, and the negative externalities of such an attack, a reliance on voluntary action on behalf of firms that provide essential services is inadequate.

Option 3: To allow competent authorities to recommend designation of 'critical dependencies' within their sector. A discretionary power will be granted to competent authorities to designate those dependencies it deems critical, in line with guidance provided by DCMS. These critical dependencies would then fall under the remit of the NIS Regulations.

This measure empowers competent authorities to require specific information from operators of essential services that is necessary to effectively manage threats to their sector through greater awareness/information access. It also grants the power to require 'critical dependencies' to demonstrate that they are taking appropriate and effective measures to prevent and mitigate the effect of a cyber attack.

Option 3 is the preferred option of this measure.

Measures to amend the incident report duties of organisations in scope beyond the limit of continuity of service

Option 1: Do nothing

Doing nothing is not an acceptable option. Close to zero incidents have been reported formally under NIS since the regulations came into force. This is in stark contrast with the numbers obtained informally, i.e. through voluntary and media reporting. This is a clear indication that the incident framework has severe limitations and is not correctly serving its intended purpose : to gather actionable intelligence. As a result, competent authorities have a poor picture of the threat landscape and are not equipped with the adequate information needed to take corrective and/or preventative measures. Amending the reporting framework to reflect actual incidents will

help competent authorities ensure that businesses are taking appropriate action to mitigate the risks of their essential service being disrupted.

Option 2 : Encourage competent authorities to include voluntary reporting of these incident types within their sectoral guidance

This is already being pursued in the majority of the NIS sectors (e.g. the water sector), with regulators stating clearly via guidance that the companies will not be penalised for voluntarily submitting information. However, regulators have found that regulated entities still do not report these incidents. Given that there is no explicit legal obligation to comply, companies prefer to withhold information about such incidents. This is likely in order to prevent regulators from discovering vulnerabilities in the regulated bodies' NIS systems, and consequently asking the companies to take action. This option therefore is considered non-viable.

Option 3 : Introduce the duty to report incidents that do not affect continuity of service but that have the potential to impact the service.

As stated above, amending the reporting framework is judged to be the best way to ensure that businesses are reporting incidents, and that competent authorities are able to obtain a clear picture of the extent and severity of cyber security incidents.

Option 3 is the preferred option of this measure.

Measures to allow NIS competent authorities to recover the full costs of regulatory activities

Option 1: Do nothing

This option would continue to place an undue burden on the taxpayer. The system also provides an incentive for regulated bodies to strategically delay regulators' corrective actions, in the knowledge that competent authorities only issue financial penalties as a last resort and that any interim enforcement action taken will result in large costs for the competent authority.

Option 2: Remove the limitation in the legislation and expand cost recovery to all regulatory activities. Keep the current invoice-based cost recovery model.

Option 3 : Remove the limitation in the legislation and expand cost recovery to all regulatory activities. Change the cost recovery mechanism, giving regulators the discretion to define how they recover costs (projected basis and/or recovery of historic costs) as is most appropriate for their sector.

Option 4 : Keep the limitation in legislation which prevents the recovery of enforcement activities. Change the cost recovery mechanism, giving regulators the discretion to define how they recover costs (projected basis and/or recovery of historic costs) as is most appropriate for their sector.

Options 2 and 3, which shift the total costs of NIS implementation onto industry, would help to better distribute resources by internalising the cost of regulation onto the firms that are creating

the externality. Whilst their distribution of where the costs lay for firms differs. The consultation responses and meetings with HMT will help DCMS to side for the preferred option for the final stage IA.

Policy objectives

The overarching objectives of this grouping of measures aims to make the UK more resilient against cyber security threats and to ensure that organisations that the economy is dependent on are taking appropriate steps to improve their cyber resilience. The Post-Implementation Review of NIS identified that we expect to lead to a longer-term improvement in the security of network and information systems, raising their resilience and reducing the risk posed to essential services. The security improvements by operators of essential services and relevant digital service providers, which include the security of network and information systems through strengthened standards, processes and procedure, are being made at a faster rate than would have been expected without the introduction of the NIS Regulations. The Post-Implementation Review also indicated that the regulations have led to strengthened processes for recovery from security incidents and that operators of essential services have made additional investments in their security.

Essential services create a large negative externality if they under-invest in their cyber security. These measures propose to improve the cyber resilience of more sectors than the original regulations and improve the resilience of the firms and critical dependencies of those firms already covered by the regulations.

Below a theory of change model can be seen that explains what the objectives are and how they will be met.

Theory of change

The theory of change model outlined below details how all of the measures look to meet the overarching policy objectives.

Measure	Objectives	Input	Activities	Assumptions	Output	Outcomes
The supervisory regime for DSPs	Increase cyber security among DSPs. Greater awareness of cyber risks associated with DSPs. Greater cooperation and information sharing between DSPs, regulators and end customers. Greater assurance over the cyber resilience of Digital Service Providers Increased cyber resilience in supply chains across the UK, including critical national infrastructure sectors. A stronger deterrence for threat actors to target the UK's Digital Service Providers and wider economy. Allow ICO to focus its resources on DSPs that carry the highest level of risk to the UK's cyber resilience.	Codify the two-tier differential supervisory regimes.	Increased access to expert advice from NCSC and the ICO. Organisaions may be required to invest in improving their security of network and information systems. ICO would reactively supervise vast majority of DSPs. ICO would proactively monitor and investigate the most critical DSPs to ensure they have fulfilled their duties under NIS.	There is an assumption that the proactive approach will identify areas of the organisations cyber security or recovery plan that can be improved.	Improved cyber security and a resilience to cyber attacks will decrease the risk that RDSPs can be successfully attacked and affected.	An improved cyber security in the economy. Fewer cyber attacks should occur and the ones that do should have a lower impact on the essential service that the DSPs and MSPs provide. A reduction in the externalities created by these firms' cyber risks.
Expand the definition of DSPs		Including more firms in the NIS Regulations, will ensure that firms take the needed steps to secure their systems.	Make firms report when an incident has occurred in their organisation that crosses the NIS threshold. Give the firms access to the ICO and the NCSC so they can access expert advice on cyber issues. Firms should increase spending on cyber security and raise its profile within the organisation, as outlined by the PIR.	It is assumed that these firms will improve their cyber security as they are designated under the NIS Regulations. This is backed up by the NIS PIR.	Improved cyber security and a resilience to cyber attacks will decrease the risk that MSPs can be successfully attacked and affected.	
Allowing the minister to update the regulations in the future	To allow the government to amend and update the NIS Regulations, within certain constraints and limitations, without requiring primary legislation.	To allow the government to amend and update the NIS Regulations, within certain constraints and limitations, without requiring primary legislation.	Change areas of the legislation, such as thresholds, appeals, reportable incidents etc.	It is assumed that these powers will be used to make the legislation adapt to the new threats posed in the cyber landscape.	Changes in legislation will be quicker than if they were done by primary legislation.	Legislation remains effective and doesn't create government failure through outdated regulations. Market failure can be better addressed.
Allowing the minister to designate sectors as part of NIS	To adress market failure created by the externalities of firms' and sectors' cyber risks quickly.	To allow the government to designate a sector or sub-sector as part of the NIS Regulations quicker than primary legislation. To reduce the cyber risks posed by sectors to the economy.	Add a sector, subsector or critical dependency that is deemed to have a large impact on the economy as part of the NIS Regulations. Make firms in that sector report incidents to the competent authority. Mandate that firms fill in compliance reporting, such as the Cyber Assessment Framework. Give firms support through competent authorities and the NCSC relating to cyber security. Firms should increase spending on cyber security and raise its profile within the organisation, as outlined by the PIR.	It is assumed that these firms will improve their cyber security as they are designated under the NIS Regulations. This is backed up by the NIS PIR. It is assumed that these sectors will be fundamental to the UK economy.	More spending will be done on cyber security by key firms in the economy. Whilst this isn't a good outcome in itself, it is more likely to have a positive impact than negative. More firms will have cyber security as a priority at board level. More firms will be able to access NCSC and CA help on cyber incidents and their resilience plans.	Large negative externalities are not created by key firms' cyber risks. Information is also shared on risks across the sector and resilience to these risks is improved.
Allowing the minister to designate critical dependencies	To improve the resilience of the UK economy to cyber attacks by making sure that critical dependencies are required to meet a certain standard of cyber security. Reduce negative externalities created by firms' cyber risks.	Grant a discretionary power to the government to designate an organisation providing a key service or the provision of a product as being a critical dependency to the provision of an essential service under the NIS Regulationsies that the government and the relevant regulator deem to be critical, in line with subsequent guidance.				OESs and RDSPs are more resileint to indirect cyber attacks initiated through 'critical dependencies'. This will enhance the cyber resilience of critical sectors reducing negative externalities.

Measures to amend the incident reporting duties	To give authorities improved oversight/intelligence and ability to support firms when other cyber incidents occur. So incidents under NIS more closely match the breaches	To change the duties of organisations to include incidents that do not impact the continuity of service as a part of NIS.	Firms will alert the competent authorities when an incident that doesn't affect the continuity of service (threshold to be considered). This could include ransomware. Competent authorities and NCSC will be able to assess the risks posed by OESs and support the firms with these incidents.	It is assumed that there will be more incidents that will be reportable under the NIS Regulations and that firms are currently not reporting these incidents.	Increased transparency into the cyber incidents that are affecting OESs. Improved support offered by CAs on these incidents.	CAs and NCSC will have better oversight of the cyber threats facing OESs and will be able to provide more support through the NIS Regulations. Reducing the cyber risk faced by these firms in the long run.
Measures to allow CAs to recover full regulatory costs	To improve the allocation of resources by making firms pay for their own regulation. This will internalise more of the externality created by these organisations.	To give CAs the power to charge the cost created from all parts of the regulation onto those that create them.	CAs will be able to charge firms for enforcement action taken. This will make firms pay for every aspect of the regulation. CAs won't be reliant on the government to foot the bill for enforcement action.	That funding enforcement action was a factor in a lack of enforcement.	A more efficient funding mechanism where firms pay for their regulation. CAs not dependent on government money.	Funding is no longer a barrier to enforcement action. Government will also save money by not funding regulation. Externality is better internalised.

Monetised and non-monetised costs and benefits of each option (including administrative burden)

Costs

Only the costs of the preferred options have been explored in a detailed manner in this document.

The costs of these measures fall under 2 different categories; setup costs and ongoing costs. The set-up costs include: familiarisation cost; additional cyber security costs and carrying out supply chain audits. The ongoing costs include: incident reporting; additional cyber security spending; competent authority costs; compliance costs. Ongoing costs will also include costs that haven't been estimated in this Impact Assessment including the costs faced by the Computer Security Incident Response Team, which for NIS is the National Cyber Security Centre.

In table 1 below, a summary of what costs each measure will create can be indicated by a X.

Table 1: Indication of the cost types per measure

Measure	Familiarisation costs	Additional security spending	Compliance reporting	Incident reporting costs	Competent authority costs
The supervisory regime for digital service providers	*		x		x
Expanding the definition of digital service providers	x	x		x	**
Measures to allow the government to make secondary legislation to update the regulations in the future	Measures that give the government power to change the regulations, do not produce a direct cost from their enactment. Both measures give the government the power to amend the legislation. This means there will be no direct changes as a result of these measures being taken forward. For the final impact assessment an appraisal of the indirect costs and benefits will be included of these measures, to show the costs and benefits of the Secretary of State enacting these powers.				
Measures to allow the government to make amendments to the scope of NIS sectors and sub-sectors					
Measures to allow the government to designate critical dependencies that are fundamental to the provision of the essential service	x	x	x	x	
Measures to amend the incident report duties of organisations in scope beyond the limit of continuity of service	x				

Measures to allow NIS competent authorities to recover the full costs of regulatory activities	Most of the costs of regulation already fall on business, through the fees that regulators charge. The costs that currently aren't charged to business are activities covering enforcement. As there has been little to no enforcement action to date, it has not been possible to cost this measure for this IA. This is an evidence gap that will be worked on for the final IA.

*The familiarisation cost of the supervisory regime has not been monetised for this impact assessment. This is because new firms that are brought into regulation under the expansion of the definition of digital service providers will have no additional familiarisation cost, whereas those already covered by the regulations will have a small familiarisation cost. It is unknown what the split of firms will be brought under the supervisory regime.

**Work will be undertaken with the regulator to understand the cost of this regulation by the final IA.

This section of the impact assessment will first look at the set-up costs of each measure and then all of the ongoing costs for each measure. Any titles that are underlined refer to a measure title, whilst non-underlined titles refer to the cost title.

To calculate the costs and benefits, the government has used all available evidence to try to quantify the impacts of the legislative changes. Where those impacts have not been possible to quantify with the current evidence base, the government will seek to address the weaker sections of this appraisal for the final impact assessment. Where there are substantial unknowns in the calculations, the costs should be taken as demonstrative of what the costs could be. These are notably in measures that will amend the incident reporting duties and measures that will designate critical dependencies under the NIS Regulations.

The measures shall be assessed in turn and then the overlaps of the regulations will be discussed and the interactions of the impacts shall be covered in the final section.

Do nothing option (for all measures)

The baseline for this costs and benefits analysis are the regulations in their current format. The most up-to-date costs and benefits can be found in the post-implementation review of the NIS Regulations.[21] All of the measures included in this document look to build on the existing NIS Regulations. As the costs that are calculated will be incremental costs, they will be compared to a baseline cost of 0.

The base year for the appraisal period will be 2021/22. All prices presented will be presented in this base year, unless otherwise specified. The appraisal period shall be 10 years, as consistent in the Green book. For the purposes of this impact assessment, the regulations are due to be implemented at the start of 2023/24. For the final Impact assessment the timelines around implementation will be further understood and clarified.

The discount factor used to convert the values of future years into present value is 3.5%. This is taken from the Green Book.

[21] https://www.gov.uk/government/publications/review-of-the-network-and-information-systems-regulations

The number of organisations

There are currently 2 groups of organisations under the NIS Regulations. The first are operators of essential services and the second are relevant digital service providers. The latest information available on the number of organisations designated under the NIS Regulations is from the Network and Information System Post-Implementation Review. The Review found that there were 432 operators of essential services and 189 relevant digital service providers.[22]

Preferred option (for all measures)
The section below will present set up and on-going costs for each of the preferred options chosen in pages 13-17 for all 7 measures.

Set-up costs

Set-up costs - measure to expand the definition of digital service providers

Number of firms

Expanding the definition of digital service providers aims to regulate the medium and large managed services providers operating in the UK. The National Cyber Security Centre estimates that there are 3,500 managed service providers operating in the UK. As this regulation could be overburdensome to small and micro businesses, DCMS aims to exclude them from the regulations. To estimate the number of medium and large organisations that would fall into scope of the NIS Regulations, DCMS have looked at the managed service providers that hold managed service contracts with the government. DCMS found that 56% of managed service contracts are held by small and micro businesses. It is therefore estimated that there are currently 1,500 managed service providers[23] that would be brought under the regulations as part of the measure to expand the definition of digital service providers. As this number could grow or shrink throughout the appraisal period, 3 scenarios have been presented. A low case of 1,000 and a high case of 2,000 have been used to show the effects of a change in the number regulated, this will also capture the small number of small and micro businesses, if any, that may be designated under the regulations.

Familiarisation costs

The digital service providers that will be brought under the NIS Regulations for the first time will have a cost associated with the familiarisation of the regulations. The post-implementation review of NIS did not update the familiarisation costs of the NIS Regulations, so the costs have only been updated to reflect the increase in wages since the original NIS Regulations Impact assessment. The table below is an updated version of table 2 in the NIS Post-implementation Review. The updated hourly wages have been taken from the ONS Annual Survey of Hours and Earnings (ASHE) 2020. These hourly wages have been inflated into 2021/22 prices through the Office for Budget Responsibility's GDP Deflators, in line with Green Book Guidance. The

[22] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/960574/CCS207_CCS0320329850-001_Network_and_Information_Systems_Regulations_Post-Implementation_Review_Web_V2.pdf

[23] Rounded to the nearest 100. DCMS is considering the option of allowing the ICO to designate specific small and micro-businesses providing digital services within the scope of NIS. However, these have not been included as DCMS is currently gathering evidence on the impact of relaxing the small and micro exemption through the public consultation process. The evidence collected will be reflected in the final impact assessment.

number of hours required from a legal professional and a information technology and telecommunications director has been taken from the original NIS Impact assessment.

Table 2: Familiarisation costs, ONS ASHE 2020 provisional figures.

	Number of hours for familiarising with legislation	Number of hours for guidance documents	Hourly wage 2020 ASHE provisional (£) (2020/21 prices)	Total cost per organisation, incl overhead charge (22%[24])
Legal professional	6	6	£26.35	£393.92
Information technology and communications directors	3	3	£35.02	£261.77

When scaled by the estimated 1,000 to 2,000 medium and large managed service providers, the total cost generated is between £656,000 and £1,311,000 with a central scenario of £984,000[25] (in 2021/22 prices). This cost is assumed to be incurred in the first year of the regulations 2023/24. In present value the familiarisation cost of expanding the definition of digital service providers is between £611,000 and £1,221,000 with a central scenario of £916,000[26].

Additional cyber security spending

The NIS Post-Implementation review provided good detail on the increase in cyber security spending that organisations have undertaken as a result of the NIS Regulations. The surveys asked respondents how much they have spent on 3 separate areas of cyber security, including physical security, internal staff costs and external costs. Their responses were used to update the cost and benefit analysis from the original IA[27].

It was estimated that each firm spent between £43,750 and £50,000 each in 2016 prices, as a result of the regulations. This figure has been inflated to 2021/22 prices, costing each organisation an estimated £48,240 to £55,131. As the 1,500 firms will be brought under the regulations for the first time, it is assumed that they will all incur these costs in the first year of the regulations. This creates a total cost of between £48,240,000 and £110,263,000 in 2021/22 prices. As with other set-up costs, this is assumed to be incurred in 2023/24. The present value of this expense is between £44,922,000 and £102,679,000.

[24] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/827926/RPC_short_guidance_note_-_Implementation_costs__August_2019.pdf

[25] To the nearest 1,000.

[26] To the nearest 1,000.

[27] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701054/Network_Information_Systems_Directive_Final_Impact_Assessment.pdf

Set-up costs - measures to allow the government to designate critical dependencies that are fundamental to the provision of the essential service

Number of firms

As DCMS does not yet know how many firms are likely to be critical dependencies, the costs shown in this section are just demonstrative and therefore have not been included in the EANDCB and the NPV. The supply chains of operators of essential services are not something that is publicly available. To address this evidence gap, DCMS is commissioning research that will help to understand the likely impacts of designating critical dependencies.

To demonstrate the impacts, DCMS has assumed that this policy will apply to all the firms under the NIS Regulations. This means the policy will apply to all 2,111 that are estimated to fall under the NIS Regulations.

Other set-up costs

Firms will firstly be required to report to the competent authorities their critical suppliers. This will be an exercise that will require administrative work to send the suppliers in the required format. There are a few critical assumptions that are unknown to estimate this cost: the first is the number of suppliers each firm has; and the second is the amount of time it will take per supplier to submit the documentation.

As mentioned above, to demonstrate the costs DCMS has included some assumptions. The first being the number of suppliers each firm has. It has been assumed that there will be a low number of 100 suppliers per firm and a high number of 10,000 suppliers per firm. The central estimate will be 1,000 suppliers per firm.

For the amount of time taken to submit the information for each supplier, it has been assumed that it will take between 10 and 210 minutes per supplier to complete the return. The central scenario is that it will take 110 minutes per supplier. Both the assumptions of the number of firms and the time taken to submit the information will be covered by the research that DCMS is commissioning.

The wage used to estimate the cost of filling in this cost of filling in the return is that of a buyer and procurement officer, taken from the ONS ASHE 2020 provisional estimates. This wage was then uplifted into 2021/22 prices using the OBR's GDP Deflators. The table below demonstrates the cost of completing the supplier return.

The low, central and high scenarios have been taken from the number of managed service providers that will be included in the regulations from the analysis above. DCMS has opted to show sensitivity through all the other measures.

Table 3: Firm cost of completing the supplier audit.

	Low	Central	High
Number of NIS Organisations	1,611	2,111	2,611
Number of suppliers per organisation	100	1,000	10,000
Time taken per supplier to complete the return (minutes)	10	110	210
Wage of a buyer and procurement officer (in 2021/22 prices, including 22% overheads)	£18.70	£18.70	£18.70
Total cost in 2021/22 prices	£502,000	£72,370,000	£1,708,854,000
Total cost in present value	£485,000	£69,837,000	£1,649,044,000

The costs above will be a direct cost to business.

There will be some set-up costs to the competent authorities and DCMS as which critical dependencies are included in the NIS Regulations are decided upon. These costs are very uncertain but are likely to be limited. Before estimating how much the costs to the government will be, DCMS will conduct the research of what the critical dependencies look like and how the process of designating a critical dependency will work. A full assessment of these costs will be included in the final IA.

Familiarisation costs

The new firms that are brought under the NIS Regulations are likely to be fewer than are currently under the regulations. DCMS has created 3 scenarios for the number of critical dependencies that will be brought under the regulations. These scenarios are 5%, 10% and 15% of the firms currently regulated by NIS will be added to the regulations. This means the number of critical dependencies for this scenario based assessment will be 81, 211 and 392 for the low central and high cases respectively.

These firms will face the same familiarisation costs outlined in the measure to bring the managed service providers under the NIS Regulations and can be found in table 2. The total costs of this number of firms being brought under the regulations is between £19,000 and £270,000 with a central scenario of £97,000 in 2021/22 prices.

Additional cyber security spending

As mentioned in the expanding the digital service providers costs, there will be an increase in the new firms that are brought under the legislation. These costs will be between £43,750 and £50,000 for each new firm in 2016 prices, as a result of the regulations. This figure has been inflated to 2021/22 prices, costing each organisation an estimated £48,240 to £55,131.

When this is applied to the number of new firms brought under this measure, there will be an additional spend on cyber security of £3,907,000 and £21,611,000 in 2021/22 prices. This equates to a present value between £3,639,000 and £20,125,000.

Set-up costs of measures to amend the incident report duties of organisations in scope beyond the limit of continuity of service

As the guidance of what is reportable under the new proposed duty is or what will be reportable has not been drafted at this stage in the legislative process, DCMS have made the assumption that it will take around half the time of the original NIS guidance for the existing firms that will be covered by the regulation. For new firms that are brought under the regulation, such as those in expanding the definition of digital service providers, there will be no additional familiarisation time, as the format of the guidance they read will include the reporting of near misses. As noted above, the number of firms that are already under the regulations are estimated at 611 firms. Table 4 below highlights the familiarisations costs per firm of changing the incident reporting duties.

Table 4: Familiarisation costs, ONS ASHE 2020 provisional figures.

	Number of hours for familiarising with legislation	Number of hours for guidance documents	Hourly wage 2020 ASHE provisional (£) (2020/21 prices)	Total cost per organisation, incl overhead charge (22%[28])
Legal professional	3	3	£26.35	£196.96
Information technology and communications directors	1.5	1.5	£35.02	£130.88

When scaled by the estimated 611 existing firms, the total cost generated is £200,000[29] (in 2021/22 prices). This cost is assumed to be incurred in the first year of the regulations 2023/24. In present value the familiarisation cost of changing the incident reporting duties is £187,000[30].

[28] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/827926/RPC_short_guidance_note_-_Implementation_costs__August_2019.pdf

[29] To the nearest 1,000.

[30] To the nearest 1,000.

On-going costs

<u>On-going costs - measure to introduce supervisory regime for digital service providers</u>

The number of firms that will be brought under the supervisory regime for digital service providers is currently not known. DCMS will do an assessment of the likely number of firms for the final IA. For the purposes of this IA, 3 scenarios have been used. The central estimate is 60 firms will be brought under the supervisory regime with the low and high being 30 and 100 firms respectively. This measure has no knock on impacts to other measures, so these scenarios are only used in this section.

Compliance costs

As policy design is still ongoing, the below assessment outlines the cost impact of 3 scenarios, which are most likely to be pursued for the supervisory regime for digital service providers. The central scenario is 60 firms in a proactive supervisory regime, with a low and high scenario of 30 and 100 respectively.

The costs incurred by the organisations under proactive regulation will relate solely to the compliance cost of reporting to the competent authorities. These organisations will either be currently regulated under the NIS Regulations or be brought into the regulations through a different measure, namely the expansion of the definition of digital service providers. This means the other costs of the NIS Regulations have either been covered in previous impact assessments or in other sections of this impact assessment. There will be no familiarisation cost of the regulation as it is assumed that no organisation is unaware of their obligations under NIS. These costs were set out in the final impact assessment of the NIS Regulations and were not updated by the NIS Post-Implementation Review.

The final impact assessment covered the cost of completing any additional compliance assessments, these assessments will require both a Lawyer and a senior manager to complete the assessments. The time it takes these employees to complete the assessments deviates by firm size. The table below only shows the costs by size of the firm.

Table 5: Compliance cost to business

Number of hours	Small/Micro	Medium	Large
Legal professional	1.5	5	10
Senior manager	2	7	14
Staff cost of compliance			
Legal professional (2021/22 prices)	£40	£132	£264
Senior manager (2021/22 prices)	£70	£245	£490
Total cost per organisation per year (2021/22 prices)	£110	£337	£754

As the proportion of firms that are small/micro, medium and large is not known at this stage of policy development, an average cost will be taken between the medium and large firms, as small and micro firms will likely only make a small percentage of the firms, if included at all.[31] DCMS will do further research and policy development to understand the likely proportion of medium and large firms for the final impact assessment.

For the total cost of reporting to the regulator, the annual cost is multiplied by the number of firms and then multiplied by the number of years. In 2021/22 prices this generates a cost of £170,000, £339,000 and £565,000 for 30, 60 and 100 firms respectively over a ten year period. In present value this equates to between £135,000 and £451,000 with a central scenario of £270,000.

Costs of competent authorities

The Information Commissioner's Office has provided DCMS with an estimated cost of providing regulation to 30, 60 and 100 firms, as it is unknown how many digital service providers will be designated to complete the compliance reviews under the NIS Regulations. These costs are on-going costs, so to cover the full 10 years, DCMS has made the assumption that the costs will be constant in 2021/22 prices. Table 6 below shows the costs to the competent authority over the 10 year appraisal period.

Table 6: Competent authority costs of proactive regulation in 2021/22 prices.

Year	**Low - cost of regulating 30 firms**	**Medium - cost of regulating 60 firms**	**High - cost of regulating 100 firms**
2023/24	£1,004,708	£1,714,716	£2,956,559
2024/25	£1,004,708	£1,714,716	£2,956,559
2025/26	£1,004,708	£1,714,716	£2,956,559
2026/27	£1,004,708	£1,714,716	£2,956,559
2027/28	£1,004,708	£1,714,716	£2,956,559
2028/29	£1,004,708	£1,714,716	£2,956,559
2029/30	£1,004,708	£1,714,716	£2,956,559
2030/31	£1,004,708	£1,714,716	£2,956,559
2031/32	£1,004,708	£1,714,716	£2,956,559
2032/33	£1,004,708	£1,714,716	£2,956,559
Total	**£10,047,080**	**£17,147,160**	**£29,565,590**

[31] DCMS recognises that any relaxation of the small and micro firm exception must be proportionate to risk. Evidence is therefore being gathered through the public consultation process on the impact of relaxing this exemption, and this will be reflected in the final impact assessment.

It is assumed that these costs will fall on businesses, as these costs are already recoverable under the NIS Regulations. However, the government will continue to work closely with the regulator to ensure appropriate support is in place.

On-going costs - measure to expand the definition of digital service providers

Incident reporting costs

As part of their obligations under the NIS Regulations, firms will be required to report cyber incidents that are above the threshold to their competent authority. This is the same practice as the current NIS Regulations. The NIS Post-Implementation Review was not able to update the costs of the NIS Impact Assessment for incident reporting costs, as it was unclear whether firms responded on an annual or per incident basis. The cost per incident in 2016 prices was £54. Using the OBR GDP deflators this has been uplifted into 2021/22 prices, the cost per incident for this appraisal is £59.54.

The number of incidents that the 1,500 new firms will generate, is assumed to be a consistent rate as the previous firms regulated under the NIS Regulations. As the Post-Implementation Review was unable to update the number of incidents per year, the same number of incidents per firm will be used as the original IA. In the low case, it was estimated that there would be 39 incidents per year across the 621 companies, totaling a rate of 0.06 reportable incidents per company. When applied to the 1,500 new organisations, this creates a total of 94 new incidents per year, with 1,000 firms producing 63 incidents per year and 2,000 producing 126 incidents per year.

The high case there was estimated to be 222 incidents across the 189 relevant digital service providers under the NIS Regulations. This produces an incident rate of 1.17 incidents per relevant digital service provider. By using the same methodology as the previous paragraph, the number of incidents that the new 1,500 firms that are regulated by the legislation will produce is 1,762 incidents per year, with 1,000 firms producing 1,175 incidents per year and 2,000 firms producing 2,349 incidents per year.

The total impact of the cost of reporting incidents of the new 1,500 firms brought under the regulation is estimated to be between £56,000 and £1,049,000 over the 10 year appraisal period in 2021/22 prices. The low scenario of 1,000 firms producing 63 incidents per year, produces a cost of £37,000 in 2021/22 prices and the high scenario of 2,000 firms producing 2,349 incidents per year costs £1,399,000 in 2021/22 prices. The present value range of this increase in incident reporting cost is £32,000 and £1,203,000.

Whilst during Covid-19 the number of cyber crimes occurring has increased as criminals' behaviours change[32], there has not been an increase in the serious incidents that would be recorded under the NIS Regulations. The NIS Post-Implementation Review also noted that the number of incidents had been lower than initially forecast, so it is likely that this will be an overestimate.

Additional cyber security spending

Whilst some of the additional cyber security spending will include set-up costs such as, additional spending on physical security, there will also be an increase in staff costs for the

32 https://www.theguardian.com/technology/2021/may/10/uk-covid-related-cybercrime-fuels-15-fold-rise-in-scam-takedowns

security. From results taken from the NIS Post-Implementation Review, it is estimated that relevant digital service providers spend approximately £100,000 per firm per annum in 2016 prices. In 2021 prices this equates to approximately £110,000. When multiplied by the number of firms in the 3 scenarios, this equates to £1,102,626,000 to £2,205,253,000 in 2021/22 prices, with a central scenario of £1,653,940,000. In present value this equates to between £879,280,000 to £1,758,561,000 with a central scenario of £1,318,921,000.

On-going cost - measures to allow the government to designate critical dependencies that are fundamental to the provision of the essential service

Additional cyber security spending

Whilst some of the additional cyber security spending will include set-up costs such as, additional spending on physical security, there will also be an increase in staff costs for the security. From results taken from the NIS Post-Implementation Review, it is estimated that operators of essential services spend between £82,210 and £96,840 per firm per annum in 2016 prices. In 2021 prices this equates to between £90,640 and £106,780. When multiplied by the number of firms in the 3 scenarios, this equates to £73,421,000 to £418,564,000 in 2021/22 prices, with a central scenario of £208,277,000. In present value this equates to between £58,549,000 to £333,781,000 with a central scenario of £166,089,000.

On-going cost - measures to amend the incident report duties of organisations in scope beyond the limit of continuity of service

Increased costs of incident reports

There is currently very little understanding of how many of these incidents that do not affect the continuity of service are detected by organisations. DCMS is planning a work stream to further understand what these incidents will look like, and how many incidents there will be. The costs reported under this section are therefore purely demonstrative, and will not be included in the total costs of this IA. This will be included in the final IA.

To demonstrate the cost of this proposal, DCMS have assumed that the number of incidents will double per year. This proposal will impact a total of 2,111 organisations (1,500 managed service providers that will be included under, plus any critical dependencies that will be outlined in the next measure as to why they can't be estimated. Using the same calculations as the number of incidents that were included in the expansion of digital service providers, there will be an increase in incidents by an estimated 133 to 2,480 per annum. As the cost per incident is £59.54 in 2021/22 prices, the total demonstrative cost for incident reporting is between £79,000 and £1,476,000 in 2021/22 prices.

Other costs

As all previous work with the competent authorities and the National Cyber Security Centre (that act as the Computer Security Incident Response Team) have looked at the total costs of NIS, DCMS has not been able to assess the costs to both bodies as a result of changing the incident reporting duties. DCMS will continue its regular contact with both sets of organisations as the policy is developed, to scope out the impacts of this policy.

On-going cost -measure to allow NIS competent authorities to recover the full costs of regulatory activities

Most of the costs of regulation already fall on business, through the fees that regulators charge. The costs that currently aren't charged to business are activities covering enforcement, penalties, appeals, civil proceedings, and enforcement of penalty notices (regulations 17 to 20). As there has been very little or no enforcement action, it is very difficult to estimate what the savings to the government will be and what the cost will be to business as a result of this measure. If the post-implementation review that is due to be published next year, highlights evidence around the cost of the enforcement regime, this will be included in the final IA.

This policy will not create new costs but transfer them from government to business through the different proposed mechanisms which can be found in the policy options above. Whilst the costs of the two options will be the same by using both the hybrid system of fees and invoicing and a purely fees based system, their distribution among which firms pay for the enforcement activities will be different. DCMS are working with HMT and competent authorities to understand which of the options will result in the best outcome to meet the policy objectives.

Summary of all measures costs

Table 7: Summary of costs in present value over 10 year appraisal period

Measure	Familiarisation costs	Additional security spending	Compliance reporting	Incident reporting costs	Competent authority costs
The supervisory regime for digital service providers			£270,000		£8,012,000 - £23,577,000
Expanding the definition of digital service providers	£916,000	£927,520,000 - £1,868,824,000		£30,000 - £1,115,000	
Measures to allow the government to make secondary legislation to update the regulations in the future					
Measures to allow the government to make					

amendments to the scope of NIS sectors and sub-sectors					
Measures to allow the government to designate critical dependencies that are fundamental to the provision of the essential service	£521,000 - £1,709,124,000*	£62,456,000 - £355,392,000*	£ 335,000 - £1,621,000*	£3,000 - £274,000*	
Measures to amend the incident report duties of organisations in scope beyond the limit of continuity of service	£187,000				
Measures to allow NIS competent authorities to recover the full costs of regulatory activities					

* Costs are demonstrative due to evidence gaps and will not be included in the totals.

Due to giving the ability to recover all the costs of the regulation, businesses will bear the full cost of the regulatory activity outlined in this document. This means that all of the costs outlined in table 5 above will fall on businesses. As mentioned above, apart from the familiarisation costs of the measures to amend incident reporting thresholds, all the costs from the measures to amend the incident reporting thresholds and measures to allow the minister to designate critical dependencies will not be included in the direct costs to business (all the costs with an asterisk next to them in table 7).

Costs to government

If all the measures are implemented, the costs to the government should be very limited. Most of the regulation activities will be able to be charged to the businesses that the government regulates under NIS. As the measures are developed, DCMS will have a better understanding of whether any funding is needed to competent authorities to implement the measures.

Costs of non-compliance

In addition to these costs, firms may also have enforcement action taken against them if they do not adhere to the regulations or improvement plans. The largest fine that can be administered under the NIS Regulations is £17m. There could be other costs associated with the enforcement action such as legal costs and appeals, if applicable. This IA is unable to assess the likely costs of such enforcement action, as none has been carried out to date, so the size of fines or the incidence of such fines is unknown. These costs are outside the scope of the IA.

Total costs

The total costs that could be monetised in this appraisal of the cyber security measures are between £936,935,000 and £1,894,889,000 in present value. The EANDCB over the 10 year appraisal period is between £93,694,000 and £189,489,000, with a central scenario of £141,591,000.

Benefits

This section explores the benefits from implementing the changes to the NIS Regulations.

The overarching benefit of these measures is to improve the cyber security of the essential services that the UK economy depends upon. The average cost of a cyber incident to a business that experiences a loss of data or assets as a result of a breach is £8,460 according to the 2021 cyber breaches survey. The number of breaches that will be avoided as a result of the measures outlined in this document is not known, as it is very hard to prove a counterfactual estimate. Whilst there will be a direct benefit to business by reducing the amount of incidents or reducing the impacts to what business will suffer, there is a bigger benefit to the larger economy. To demonstrate this the economic impact of what a cyber breach could look like on an operator of an essential service, a case study will have to be used, as was used in the original NIS IA.

Case study 1: Ukraine power grid hacked

On the 23 December 2015 three power distribution companies suffered from a sophisticated cyber attack that led to 225,000 residents being without power. Power was lost for between one to six hours for the areas hit, but while the outage wasn't long more than two months after the attack control centres were still not fully operational according to experts. The attack used a number of approaches to gain access and cause disruption and destruction. While this attack is not representative of the risks to networks in the UK it does provide an indication of the scale of disruption and economic impact a successful attack can result in.

This case study highlights the negative externality that exists from poor cyber security standards of essential services. The following paragraphs detail how the measures will create a benefit and what that benefit will be.

The supervisory regime for digital service providers will improve the resilience the most critical firms in the economy have to a cyber attack. By sharing information ahead of an incident about their cyber resilience plans, the experts in the competent authorities and the National Cyber Security Centre will be able to assess whether their plans meet the standards and how they can be improved. By improving the cyber resilience plans the impact a successful breach has on both the firm itself and the wider economy is reduced. This is because firms will either face less successful breaches or will be able to recover more quickly from an attack.

It has been shown through several attacks on managed service providers the impact they have on the economy. The Kaseya Ransomware attack demonstrates the interconnectedness of these firms through other sectors of the economy, with upto 1,500 firms estimated to be impacted by the attack[33]. By bringing the most interconnected and relied upon firms into the NIS Regulations, DCMS aims to reduce the impact a cyber attack has through the supply chain by increasing the cyber security standards of these firms. This will be the benefit of expanding the definition of digital service providers, as fewer of these interconnected firms will face successful or large impact cyber breaches. The reporting of incidents also allows the National Cyber Security Centre and regulators to understand the attacks that have taken place and information can be shared to stop new types of attack becoming a threat.

The measures that give the minister the ability to amend parts of the NIS Regulations will ensure that the regulations remain effective. The threats faced in the cyber security space are constantly evolving and the regulations need to be amended quickly to keep pace with the ever changing threat. If a new threat were to emerge, the regulations could be amended more

[33] https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/

quickly than if they had to be amended by primary legislation, ensuring that cyber security standards could be changed to reflect that threat. The benefit of this is to reduce the time in which key systems could be vulnerable to new threats.

Giving the government the ability to designate sectors and sub-sectors will reduce the time between a sector being identified as having a negative externality, created by lower cyber security standards, and a being brought under the NIS Regulations. This will enable the government to rectify market failure quicker, and avoid the possibility of large losses to the economy.

As well as regulating the firms that feature in the supply chains of all sectors, DCMS proposes to regulate the firms that will regulate the critical dependencies to the NIS sectors. This will stop cyber breaches in the supply chain from being endemic across the key sectors for the UK economy. If such an attack were successful on a critical dependency in a sector such as energy, lives could be put at risk and parts of the economy could be unable to operate. By regulating these critical dependencies, the cyber security standards will be imposed on these firms and reduce the likelihood of a successful incident occurring and impacting the essential service.

Measures that will amend the reporting duties of the NIS Regulations will ensure that the regulations remain effective. This measure will allow for other types of incidents to be reported under the NIS Regulations that will enable the NCSC to have a better indication of the threats that exist. This will enable better information sharing and the potential to improve resilience or security to new cyber threats.

Other benefits that were found by the NIS Post-Implementation Review were an improved understanding of their organisations aggregate risk (56% of operators of essential services and 53% of relevant digital service providers), and 63% of operators of essential services reported that they had increased board support for cyber security in their organisation. Other reported benefits included: updated general incident management processes (48% of operators of essential services and 41% of relevant digital service providers); and sharing good practices with other operators of essential services (36% of operators of essential services and 12% of relevant digital service providers). These benefits are predicted to also occur with new firms brought under the regulations.

Risks and assumptions

Table 6: Assumptions and risks

Assumption	Risk	Mitigation
The number of firms covered by the current regulations is taken from the last post-implementation review.	Low - the number of firms is likely to have changed much since the last post-implementation review.	The next post-implementation review will give a more up-to-date figure.
The year of implementation is 2023/24.	That the legislation takes longer to implement and the year is pushed back.	None - the implementation date will be better understood by the final impact assessment. This is a low risk assumption.
Familiarisation time for the full NIS Regulations will be 6 hours for a lawyer to read and 3 for a technical director.	Low - this is based on legal advice in the last NIS IA.	None
The number of firms as proactively supervised as a result of codifying the supervisory regime that currently exists.	Medium - it is unknown just how many firms will be under the proactive regulations.	Scenario based estimates. DCMS assumed that there could be 30, 60 or 90 firms.
That the costs of regulating the relevant digital service providers in a proactive manner will be equal to the costs supplied from the ICO.	Low - as the ICO are the current regulator of relevant digital service providers, they are best placed to calculate the CA costs of the regulation.	None
Compliance costs will equal those faced by OESs.	Low - there is data to suggest that the compliance costs faced by OESs is accurate. This was both taken from the original IA and the Post-Implementation Review.	None
The number of medium and large managed service providers operating in the UK is around 1,500.	Medium - This number has assumed to stay constant throughout the appraisal period. The number could grow or shrink.	3 scenarios have been presented using the 1,500 as a baseline.
That businesses are not voluntarily reporting the cyber attacks that these measures seek to include.	Low - If firms were already reporting such cyber attacks, they would not face the costs outlined in this document but	None

	there would also be no benefit to this policy.	
The cost per incident report will be the same as the original IA.	Low - This was tested by the last Post-Implementation Review and was not changed.	This will be tested by the future Post-Implementation Review and will be displayed in the final IA.

Impact on small and micro businesses

Small and micro businesses will receive an exemption where possible from the NIS Regulations. By the nature of the regulations,small and micro businesses cannot be excluded from every measure. The measures that aim to expand the current NIS Regulations will inevitably include the small and micro businesses covered by these regulations. The number of these businesses are not known by DCMS as the last Post-Implementation Review just asked if some are regulated. The next Post-Implementation Review will ask competent authorities how many small and micro businesses are regulated under the NIS Regulations.

Codifying the existing supervisory regime for relevant digital service providers will include the most impactful relevant digital service providers in the economy to regulate.The exclusion of small and micro businesses will continue to apply by default.. However, DCMS is consulting on the option of allowing the ICO to designate specific small and micro-businesses providing digital services to be brought into scope of the NIS regulations, if they are deemed critical Even if a small or micro business were to be regulated, the additional impact of completing compliance reporting is estimated to be £110 for a small/micro business. This should not be overburdensome on a business.

For the mesure to expand the definition of data service providers, the exclusion of small and micro businesses will continue to apply by default. However, as set out above, DCMS is consulting on the option of allowing the competent authority to designate specific small and micro-businesses providing digital services to be brought into scope of NIS regulations. This could include managed service providers brought in under this measure.

The measures that would allow the crown to both change technical elements of the regulations and designate new sectors or sub-sectors is impossible to say what the impact will be on small and micro businesses as the actual changes aren't included in the legislation, just the ability to make such changes. DCMS will do an economic evaluation of any of the changes that will be made using these powers.

Changing the reporting to include other incidents could see small and micro businesses that have already been designated could face higher costs than large firms, if they see a higher number of cyber incidents. As these incidents have the potential to be a large negative externality by their impact on the wider economy, it would be proportionate to include these businesses in the regulations. To be designated under NIS the impact that a successful cyber breach will cause will be deemed large enough to not give an exemption.

A full quantification of the costs that will be borne by SMEs will be developed for the final IA.

Wider impacts (consider the impacts of your proposals)

Innovation test

DCMS is part of a trial department in government to assess the impacts of regulations on firms' abilities to innovate. As the NIS Regulations set a minimum bar for cyber security reporting, they do not limit the innovation that firms can carry out. The second post-implementation review is currently being carried out, where a set of questions has been included to understand the impact of the regulations on companies ability to innovate. These results will enable DCMS to carry out a more detailed innovation test analysis.

A summary of the potential trade implications of measure

As work is ongoing to understand the make-up of the firms that will fall under the measures outlined in this impact assessment, the possible impact on trade is not possible to understand at this stage. DCMS is commissioning work to understand what the NIS critical dependencies look like and whether this regulation will impact their ability to trade.

A full assessment of all the impacts on trade will be assessed in the final IA.

Monitoring and Evaluation

The current NIS Regulations are evaluated using Post-Implementation Reviews. The second of these reviews is due to be published in 2022. These measures will be included in any future post-implementation review of the NIS Regulations. The next post-implementation review after 2022 is scheduled for 2027; this will be enough time to compare the costs and benefits of these measures to their predicted impact.

DCMS will need to amend the questions that are posed of the regulations to capture the specific impacts of these measures separately, as they have been split out in appraisal. Both the regulated and the regulators will need to be consulted for the post-implementation review to assess the costs and benefits to the firms. Organisations that are brought under the regulations or are affected by changes to the regulations will be asked about their specific impact. To try to capture the costs of cyber attacks to the wider economy by successful attacks on operators of essential services, DCMS will need to review academic papers on the cost to the UK economy. DCMS is also working to assess the cost of cyber attacks to UK business each year. This will help to provide context to the costs of the regulations and whether they are proportionate.

For measures that give the minister power to make changes, if any changes are proposed, an economic assessment will be carried out of the proposed changes to ensure that such changes are evidence-led. These changes will also be mentioned in the post-implementation reviews of the NIS Regulations.

DCMS will have a more informed overview of cyber security across more sectors of the economy with the introduction of the managed service providers to the regulations. DCMS will be able to collect the incident data and be able to compare how incidents differ between the sectors. This will be incorporated into the next post-implementation review and an analysis will indicate whether the incidents being reported under the NIS Regulations show a closer link to the threats that are present to the essential services in the UK.

DCMS is commissioning analysis to look into the critical dependencies in the UK supply chains. This research will assess the interconnectedness of these supply chains and how cyber attacks can cross both throughout a sector and across into other sectors. This will be important both for understanding the potential benefits of the regulations, but also for the Minister deciding to adjust the scope of the regulations in future.

The additional data that DCMS will receive includes the data from changing the incident reporting duties that will be able to help improve the understanding of whether the policy is working in relation to collecting the same incidents that are frequently reported in the press but not through NIS. Whilst it will not be possible to assess if every observed incident has been reported in the press, DCMS will assess if the number of NIS recorded incidents is closer to the number of voluntarily reported incidents to the National Cyber Security Centre. This will help DCMS to understand whether the policy objective has been achieved.