GOV•UK

Department for Digital, Culture, Media & Sport

Department for Science, Innovation & Technology

Policy paper

Summary of the Bill

Updated 3 November 2026

Contents

What are we going to do?

What are the NIS Regulations?

What are network and information systems?

Why is reform needed?

What does the bill do?

Implementation

What else is government doing on cyber security and resilience?

How much will it cost?

OGL

© Crown copyright 2026

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-

licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/summary-of-the-bill

What are we going to do?

The Prime Minister said: “National Security is the first responsibility of any government, that never changes. But as the world changes, the way we discharge that responsibility must change with it.”

The Cyber Security and Resilience (Network and Information Systems) Bill will reform and add to the existing Network and Information Systems (NIS) Regulations 2018, to increase UK defences against cyber-attacks, better protecting the services the public rely on to go about their normal lives – to switch on lights, turn on the tap to safe water, and know the NHS is there to support them. The Bill will deliver a fundamental step change in the UK’s national security – making essential and digital services more secure in the face of cyber criminals and state actors who want to disrupt our way of life. The reforms will ensure the UK economy is better protected than ever, making the UK a safer and more attractive place for business.

What are the NIS Regulations?

The NIS Regulations play a pivotal role in safeguarding the services the UK public and businesses rely on every day, by placing security and resilience duties on organisations involved in the delivery of essential services and some digital services. They do not cover the whole economy. As things stand the NIS Regulations apply to:

1. Operators of essential services:

- Energy – electricity, oil, gas – e.g., energy suppliers and electricity transmission and distribution
- Transport – rail, air, maritime, road – e.g., air traffic control, traffic management and rail signalling
- Health – including NHS trusts, integrated care boards and independent providers

- Drinking water – water companies – e.g., water treatment and purification, and distribution
- Digital infrastructure – including internet exchange points and domain name system providers

2. Some digital services, including:

- Online marketplaces, online search engines and cloud computing services – some AI services may meet these definitions due to cloud and online search functionalities

These organisations must take appropriate and proportionate security measures to secure their network and information systems, and report incidents that significantly disrupt their services to their regulator (known as the competent authority).

What are network and information systems?

Network and information systems include the electronic communications systems used to allow digital communication between people or devices, such as the internet, mobile phone and wi-fi networks, and any combination of computers, software, interconnected devices, control systems, and the digital data they use or share. The NIS Regulations focus on the network and information systems that are relied on for providing an essential or digital service within scope, to keep the service running.

For example, an NHS hospital's reliance on network and information systems to carry out its services might include everything from patient record systems and diagnostic tools to staff scheduling software, internet-connected medical devices, and the IT infrastructure that keeps it all running securely. For a drinking water provider, network and information systems might include everything from water quality monitoring tools and pump control systems to customer billing platforms, systems to support internet-connected sensors in treatment plants, and the IT infrastructure that keeps operations secure and flowing.

The NIS Regulations take an "all-hazards", risk-based approach, requiring organisations to manage risks if they relate to the functioning of network and information systems relied on to provide the essential or digital service:

- Cyber security risks – protection against threats like hacking, malware, ransomware, and data breaches. For example, protecting against a threat actor gaining remote access to an organisation's control system via a phishing email.
- Physical security and broader operational resilience risks – protection from disruption from physical threats and hazards like power outages, equipment failure, human error, or environmental damage. For example, protection against a threat actor gaining access to an organisation and causing physical damage to part of a network and information system, causing disruption.

Twelve regulators (also known as competent authorities) are responsible for implementing the regulations and maintaining regulatory oversight of their relevant sector or services. The reason for this federated structure is that different sectors face different risks. The scale and nature of threats or hazards may be different for different sectors and may change over time. Different sectors can involve or be made up of different technologies which can have different vulnerabilities. The energy sector, for example, generally has a greater reliance on operational technology (e.g., turbines, substations, gas pipes) compared to the digital services sector, which is predominantly information technology-based (e.g., cloud platforms, web applications). Sector-specific nuances can make different organisations susceptible to threats in different ways and require different approaches to risk mitigation and resilience. While the government sets cross-sector duties and requirements to cover fundamental risk management and cyber hygiene, sector competent authorities then consider security and resilience in a sector-specific context, and guide, supervise and enforce in their sector.

Why is reform needed?

Technology is one of the greatest engines for creativity and innovation in modern history. It has transformed every part of our lives. Yet the systems that underpin it can be exploited by those who want to disrupt, destabilise, extort or surveil. At their hardest edge, cyber attacks can lead to unsafe drinking water, no electricity, hospitals unable to access digital patient records, and businesses unable to access their systems. This is what we must defend against.

This is not a hypothetical risk, but something playing out every day across our infrastructure and economy. In 2024, the UK was the most targeted country in Europe for cyber attacks, and looking across all cyber incidents, over 40% of UK businesses experienced cyber-attacks

(https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025) – equivalent to over 600,000 organisations. Cyber -attacks are estimated to cost UK businesses £14.7 billion each year, equivalent to 0.5% of UK GDP (https://www.gov.uk/government/publications/independent-research-on-the-economic-impact-of-cyber-attacks-on-the-uk). In the year preceding September 2025, the National Cyber Security Centre (NCSC) managed 429 cyber incidents – almost 50% (204) of which were nationally significant (https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025). This is over double the amount of nationally significant incidents from the previous year. The National Cyber Security Centre CEO warned (https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025) that, "the challenge we face is growing at an order of magnitude". An independent report (https://www.bridewell.com/insights/white-papers/detail/cyber-security-in-critical-national-infrastructure-organisations-2025) found that 95% of UK's critical national infrastructure organisations experienced a data breach in 2024.

Yet as the threat has grown more intense, frequent, and sophisticated, our defences have become comparatively weaker. The UK's only cross-sector cyber legislation (the NIS Regulations) – which protects UK essential and digital services – is out of date and insufficient to tackle the threats we face.

There have been two post-implementation reviews, one in 2020 and one in 2022. The 2020 review (https://www.gov.uk/government/publications/review-of-the-network-and-information-systems-regulations) found the regulations were raising security standards, but highlighted inconsistencies in implementation across sectors. The 2022 review (https://www.gov.uk/government/publications/second-post-implementation-review-of-the-network-and-information-systems-regulations-2018) found the regulations "are a vital framework in raising wider the UK resilience against network and information systems security threats", but that updates are required to keep pace with growing threats and new technologies, and to reflect lessons from previous incidents.

What does the bill do?

The bill has 3 pillars of reforms to update the NIS Regulations. These address current vulnerabilities, increasing the UK's defences against cyber-attacks – to protect the services the public rely on to go about their normal lives, deliver a step change in our national security, and underpin greater economic stability.

Expanded scope: The regime does not cover every UK organisation. It is about those services which are so essential, that their disruption would affect

our daily lives. The original regulations in 2018 brought into scope services like the NHS, transport system and energy network. Since then, cyber criminals are exploiting new routes – managed service providers, data centres and critical parts of supply chains – to threaten our way of life. This reflects the interconnected economy we live in, potentially causing huge disruption and financial losses to their clients. By bringing into scope more of the core services relied on across the economy, UK businesses and public services will be more secure and resilient.

- **Data centres**. From patient records to emails and financial systems, data centres are critical to nearly all economic activity and public services. Data centres will be classed as essential services, and data infrastructure as a NIS sector. Medium and large data centres and enterprise data centres meeting the thresholds will be required to have appropriate and proportionate measures in place to manage risks. Ofcom will serve as the operational regulator.
- **Managed service providers**. Many companies now outsource their IT services to managed service providers, who may provide IT helpdesks and cyber security services. They have unprecedented access to their customers' systems, making them an attractive target that cyber actors increasingly exploit. Medium and large managed service providers will be brought into scope, ensuring they adhere to robust cyber security practices. The Information Commission will be the regulator.
- **Large load controllers**. Load controllers are organisations managing electrical load for smart appliances, e.g., to support electric vehicle (EV) charging during peak times. They are a vital tool as the UK transitions to Clean Power 2030 and Net Zero. Large load controllers will be brought into scope, reducing the risk of grid disruption through enhanced cyber security requirements.
- **Designated critical suppliers**. In June 2024, a supplier of pathology services to the NHS was victim of a cyber attack which caused over 11,000 postponed appointments and procedures, and, tragically, contributed to the death of a patient. A single supplier's cyber vulnerability can severely affect vital public services and are now increasingly exploited by those who intend to do us harm. Much like the financial services sector's critical third parties regime, regulators will be able to designate critical suppliers, ensuring the most important suppliers to essential and digital services are subject to the regulatory regime.

Effective regulators: 12 regulators are responsible for implementing these laws. This allows for a sector-specific approach, as different organisations are vulnerable to threats in different ways, such as through the technology they use. The bill will drive a more consistent and effective regime, with expanded and more timely reporting of harmful cyber attacks, a stronger mechanism for

government to set priority outcomes for regulators to work to, and a fuller toolkit for sharing information, recovering costs and enforcement.

- **Incident reporting**. The current regime means that regulators only get informed about cyber incidents if they have caused significant disruption. But this does not include instances where there has not yet been significant disruption to services – like hospitals having their systems hacked by cybercriminals who wait to lock the hospital out and demand payment in return. Reporting of more harmful cyber breaches, quickly, is essential. Through the bill's reforms, more forms of harmful cyber breaches will need to be reported to regulators, where they have the potential to cause significant impacts, with initial notification within 24 hours and a fuller report within 72 hours. NCSC will be informed at the same time. And to ensure their clients can protect themselves as well, data centres and digital and managed service providers will need to inform their customers if they are likely to have been impacted.
- **Statement of strategic priorities**. Having different regulators for different sectors means they can apply their expertise and account for sector specific risks. But we recognise the implementation and success of the regime has been inconsistent, leading to some sectors being relatively more vulnerable to hostile activity and disruption. The Secretary of State will be given powers to drive better consistency in how regulators implement the NIS Regulations through setting the priority outcomes regulators will have a duty to seek to achieve. These outcomes will be set out in a designated public statement of strategic priorities, a well-used tool across a range of regimes, such as online safety, helping regulators consider how they can support government to achieve its strategic priorities.
- **Cost recovery**. Currently, regulators are constrained in their ability to recover the costs associated with overseeing and enforcing the regime which keeps our essential services safe. Regulators will be empowered to recover the full costs associated with their NIS duties, so they are better resourced to carry out their responsibilities. But they will also be required to show how these funds are being used, and in accordance with new charging schemes, giving more transparency and predictability for businesses being charged.
- **Information sharing**. The ability to share information is fundamental to the successful functioning of the regime. This helps regulators, the UK intelligence agencies and law enforcement develop a consistent and comprehensive understanding of cyber risks and mitigations, and reduces administrative burdens for businesses. Greater clarity will be provided on what information regulators can share and receive, including with law enforcement, to support delivery of NIS functions and wider cyber security and resilience while minimising burdens on businesses.

- **Enforcement**. The existing enforcement regime is not as effective or clear as it could be, risking non-compliance. The maximum financial penalty will be amended – enabling potentially higher penalties when appropriate and proportionate – to reflect the significance of the regime and align with comparable legislation, such as General Data Protection Regulation (GDPR) laws and those which protect the cyber security of products, like baby monitors and smartphones. Penalty bands will also be simplified to make them clearer, and the regime more effective.

Enabling resilience: The government no longer has powers to head off the threats faced by the UK as they change and evolve. That is why the government will be given the tools to quickly strengthen our cyber security and resilience in response to the ever-changing threat landscape, and respond to imminent threats to our national security and way of life.

- **Future-proofing**. The government will be more agile and responsive to evolving to cyber threats with powers to make changes to the regime in secondary legislation, such as bringing more sectors into scope, or updating and introducing new security and resilience requirements. This fills a gap following Brexit - and will be key to implementing the regime.
- **Powers of direction**. Geopolitical or technological developments could lead to rapid increases in the cyber threat. Drawing from similar national security regimes in the UK, the government will be able to direct regulators or regulated entities to take targeted and proportionate action in response to imminent threats that risk UK national security.

Implementation

The government will coordinate a sequenced approach to implementation, bringing the bill's reforms online as soon as possible, while also giving affected industry and regulators appropriate information and time to plan, prepare, and adjust practices. A business adjustment period will be communicated prior to new or updated duties coming into force.

The bill will come into force in phases once it has become an Act. Certain measures will come into force on Day 1 or on Month 2 following Royal Assent, while others will be brought into force through future secondary legislation (also known as "commencement regulations"), at a time determined by the Secretary of State. These have been set out below as a non-exhaustive list:

Day 1

- Future proofing
- The post-implementation review

Month 2

- Statement of strategic priorities
- Information sharing

Via secondary legislation

- Powers of Direction
- Data Centres
- Relevant Managed and Digital Service Provider updates
- Large Load Controllers
- Critical suppliers
- Incident reporting
- Cost recovery

Most of the measures that will come into force via secondary legislation rely on further detail to be operational and implemented. These are technical details and measures that are not appropriate for primary legislation and so would be introduced in secondary legislation following consultation (please see the Futureproofing factsheet (https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/futureproofing) and the factsheets (https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets) for other measures for more details).

The introduction of this secondary legislation will be coordinated in order to ensure that all relevant duties and information are in place and available before compliance begins for existing and newly regulated entities.

For some areas, such as Relevant Managed Service Providers, relevant digital service providers and data centres, we have set timeframes and procedures for registering with the relevant regulator once their provisions are in force. Further detail on this is set out in the Data Centres (https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/data-centres) and Relevant Managed Service Providers factsheets (https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/relevant-managed-service-providers), respectively.

This phased approach will allow time for government to consult stakeholders on its wider implementation approach and policy to be included in secondary legislation, where necessary. We intend to consult on implementation proposals in 2026. We will then analyse and incorporate feedback, as well as consider any relevant developments during bill passage and the wider cyber and risk landscape. A government response to the consultation will be published and then secondary legislation will be laid before Parliament. Relevant stakeholders will be given an appropriate adjustment period.

What else is government doing on cyber security and resilience?

The government is clear that decisive action is required to tackle the increasing cyber threat, to protect the public and the economy, and maximise the opportunities to the UK from our domestic cyber sector.

The Cyber Security and Resilience (Network and Information Systems) Bill is part of the government's wider strategy to improve UK cyber defences. It will also sit alongside existing legislation, including sector specific legislation such as the Telecommunications Security Act 2021 and Financial Services and Markets Act 2023.

More broadly, the government's planned National Cyber Strategy refresh will articulate the government's vision – and agreed collective action in partnership with businesses, devolved governments, regulators, law enforcement and the public – to head off the proliferating cyber threat, strengthen the UK's cyber security and resilience, and maximise growth opportunities from the UK cyber sector. It will also demonstrate that the UK remains a global leader on cyber – taking a proactive, strategic, and collaborative approach to securing national interests in an increasingly complex digital world.

Ahead of this and alongside the Cyber Security and Resilience Bill, further action is already being taken to strengthen the cyber security and resilience of the UK, including:

1. More support and guidance for businesses, so organisations of all sizes know what good looks like. We are driving uptake of 5 basic controls called Cyber Essentials, recently launched a package of support for board members and directors – the Cyber Governance Code of Practice (https://www.gov.uk/government/publications/cyber-governance-code-of-practice/cyber-governance-code-of-practice), and to support Secure-by-Design technology we have issued codes of practice for apps and app stores, software, and artificial

intelligence. NCSC has a range of guidance available on its website, including the recent launch of Cyber Assessment Framework version 4.0 (https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf)

2. Protecting our national interests in cyber space, with the UK a leading responsible cyber power within NATO. This includes the National Cyber Force, which continues to deliver offensive cyber operations to counter threats from hostile states, terrorists, and serious cyber criminals.

3. Maximising the strengths of the UK cyber security sector as a driver of economic growth and innovation – building on recent year on year growth of the £13.2 billion UK cyber sector and boosting the existing 67,000 jobs. To this end, the government is supporting, promoting, and growing the UK cyber security sector, including through a pre-seed accelerator programme – Cyber ASAP, as well as supporting home grown cyber skills through initiatives like TechFirst.

4. The government is working with international counterparts to drive global cyber security and resilience. This includes the security and defence partnership between the European Union and the UK, agreed in May 2025, which set out that thematic dialogues will be conducted on cyber issues, given the interconnectedness and interdependence of UK and EU security and prosperity.

Economy-wide support and guidance

Organisations across the whole economy benefit from free guidance and support from NCSC and government. This covers all sectors e.g. food, retail, wastewater and space.

Sector-specific regulatory frameworks

Network and Information Systems Regulations 2018 (https://www.legislation.gov.uk/uksi/2018/506): Requires organisations in scope to have robust cyber security practices. Covers:

- energy
- transport

- health
- drinking water
- digital infrastructure
- some digital services

and will be expanded by the Cyber Security and Resilience Bill to include:

- data centres
- managed service providers
- large load controllers

Other regulatory frameworks: Such as the Telecommunications Security Act (https://www.legislation.gov.uk/ukpga/2021/31/contents) and Financial Services and Market Act (https://www.legislation.gov.uk/ukpga/2023/29/contents), setting specific security and resilience duties for sectors.

How much will it cost?

An impact assessment has been published to assess the costs and benefits of the bill to businesses and other stakeholders (https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-supporting-documents). Our impact analysis shows the cost of this legislation is estimated to be less than £150 million per year.

12 regulators implementing the NIS Regulations

Operators of Essential Services: Sector	Operators of Essential Services: Sub-sector	Regulator in England	Regulator in Wales	Regulator in Scotland	Regu in North Irela
Energy	Electricity	DESNZ and Ofgem	DESNZ and Ofgem	DESNZ and Ofgem	Depa of Fir

Operators of Essential Services: Sector	Operators of Essential Services: Sub-sector	Regulator in England	Regulator in Wales	Regulator in Scotland	Regu in North Irela
Energy	Large load controllers (new)	DESNZ and Ofgem	DESNZ and Ofgem	DESNZ and Ofgem	Depa of Fir
Energy	Gas	DESNZ and Ofgem	DESNZ and Ofgem	DESNZ and Ofgem	Depa of Fir
Energy	Oil	DESNZ	DESNZ	DESNZ	Depa of Fir
Transport	Maritime	DfT	DfT	DfT	DfT
Transport	Air	DfT and CAA	DfT and CAA	DfT and CAA	DfT a CAA
Transport	Rail	DfT	DfT	DfT	Depa of Fir
Transport	Road	DfT	DfT	Scottish Ministers	Depa of Fir
Health	Healthcare	DHSC	Welsh Ministers	Scottish Ministers	Depa of Fir
Drinking water	Drinking water	DEFRA	Welsh Ministers	Drinking Water Quality Regulator	Depa of Fir
Drinking water	Drinking water	Drinking Water Inspectorate	Drinking Water Inspectorate	Drinking Water Quality Regulator	Depa of Fir
Digital infrastructure	Inc. internet exchange points and domain name	Ofcom	Ofcom	Ofcom	Ofco

Operators of Essential Services: Sector	Operators of Essential Services: Sub-sector	Regulator in England	Regulator in Wales	Regulator in Scotland	Regu in North Irela
	system providers				
Digital infrastructure	(new) Data infrastructure	Ofcom	Ofcom	Ofcom	Ofco

Digital and managed services: Sector	Regulator in England	Regulator in Wales	Regulator in Scotland	Regulator in Northern Ireland
Relevant digital service providers (RDSP)	ICO	ICO	ICO	ICO
Relevant managed service providers (RMSP) (new)	ICO	ICO	ICO	ICO

OGL

All content is available under the Open Government Licence v3.0, except where otherwise stated

© Crown copyright