Cyber Security and Resilience Policy Statement to strengthen regulation of critical sectors

New proposals will combat the growing threat to UK critical national infrastructure (CNI).

Jonathon Ellison

Cyber Security & Resilience Bill introduced

The Cyber Security and Resilience Bill was introduced to Parliament on 12th November 2025. Read the full announcement from DSIT

As the NCSC's Director of National Resilience, when the government announced it was bringing a Cyber Security and Resilience Bill before parliament in July 2024, I considered it a landmark moment in tackling the growing cyber threat to vital services such as water, power and healthcare. That's why today we welcome the publication of the Department of Science, Innovation and Technology's (DSIT) **Cyber Security and Resilience Policy Statement** which sets out a series of legislative proposals that will help tackle the increasingly prolific and diverse cyber threats to the UK.

Tackling the 'widening gap'

As Richard Horne, the NCSC CEO, outlined in his speech to mark the launch of the 2024 NCSC Annual Review:

> *there is an ever widening gap between, on the one hand, the threat and our exposure to it and, on the other, the defences that are in place to protect us*

We are certainly seeing more frequent, sophisticated and intense hostile activity in UK cyberspace, and there is global evidence that critical systems make attractive targets for hostile states and malicious cyber actors.

Just as in all modern digital economies, the UK's critical systems are reliant on our online infrastructure. Hostile actors are increasingly exploiting this dependence, conducting cyber attacks that cause maximum disruption and destruction. For example, the June 2024 cyber attack on Synnovis – which impacted critical health services in the UK – demonstrated how fundamentally reliant our health services are on online technology.

The Network and Information Systems Regulations 2018 (NIS Regulations) – the UK's only cross-sector cyber legislation – went some way to enhancing the security of UK critical networks and information systems. But the capabilities of our adversaries are growing, which means we now need to use legislative and regulatory tools to further raise our cyber security and resilience. The Telecoms Security Act of 2021 demonstrated the benefit of introducing regulation in response to the changing threats in this sector.

How will the proposed legislation address the growing cyber threat?

The legislative proposals announced by DSIT today will play a critical role in closing the widening gap between the cyber threats we face and our ability to defend against them.

If these proposals are adopted:

Broader scope for the NIS Regulations

More organisations and suppliers would be brought into scope of the NIS Regulations, including data centres, Managed Service Providers (MSPs) and critical suppliers, ensuring more organisations are subject to this strengthened framework.

More tools for regulators

Regulators would have more tools to improve cyber security and resilience in the sectors they regulate. A broader range of significant cyber incidents would need to be reported to regulators.

Flexibility to update framework

The government would have greater flexibility to update the framework as and when needed, to respond in an agile way to changing threats, for instance by extending the framework to new sectors.

New executive powers

The government would have new executive powers to respond to cyber threats, when it's necessary for national security.

Taken together, DSIT's legislative proposals represent a significant uplift in the regulatory framework for CNI cyber security. The NCSC is supportive of the additional measures under consideration that would give the UK some of the strongest protections in the world against advanced attackers targeting our CNI. As we face potentially volatile geopolitics in the years ahead, these measures will play an important role in safeguarding our essential services.

How will the NCSC help?

One aspect of the NCSC's role is to raise awareness of the cyber threat to the UK, and to guide citizens and organisations towards trusted cyber security advice, tools and services – promoting best practice, preparedness and mitigation. The NCSC also plays an important role in strengthening the country's cyber ecosystem, supporting its growth and cultivating talent.

The proposals announced today will bolster the regulatory framework, ensuring more effective and consistent application across the different NIS-regulated sectors. NCSC resources will support this in the following ways:

- The NCSC **Cyber Assessment Framework (CAF)** will support those operators of essential services, and digital service providers and critical suppliers in scope of the NIS Regulations, in managing and assessing their cyber risk.
- The **Cyber Resilience Audit scheme** and the **Cyber Essentials** assessment service – complementary offerings to the CAF – enable industry professionals to provide independent evidence against the CAF outcomes. They offer resources that regulators can use to improve resilience and cyber security in their sectors.

What next?

These legislative proposals offer a real opportunity to tackle the increasing acceleration and diversification of cyber threats to UK critical sectors. We will work closely with DSIT, colleagues across government, and our partners in industry and the wider cyber ecosystem, as the proposals are further developed and implemented. We encourage those organisations likely to be affected by these proposals to familiarise themselves with the detail in the DSIT **Cyber Security and Resilience Policy Statement**.

Jonathon Ellison, NCSC Director of National Resilience

WRITTEN BY

Jonathon Ellison
NCSC Director of National Resilience

PUBLISHED

1 April 2025

PART OF BLOG

NCSC publications