Department for
Science, Innovation
& Technology

Feryal Clark MP
Parliamentary Under-Secretary of State for AI and Digital Government
Department for Science, Innovation and Technology
100 Parliament Street,
London,
SW1A 2BQ

Chi Onwurah MP
Chair of the Science, Innovation and Technology Committee
House of Commons
London
SW1A 0AA

1 April 2025

Dear Chi,

CYBER SECURITY AND RESILIENCE BILL: POLICY STATEMENT

I am writing regarding the Cyber Security and Resilience Bill (the Bill) to inform you of our intent to publish a policy statement, which will be laid before Parliament today.

The statement will set out the proposed legislative measures for the Bill, ahead of its introduction to Parliament later this year.

The Bill will represent a significant step forward in our legislative efforts to protect the UK from the growing threats of cyber-attacks. The current cyber security regulations reflect law inherited from the EU, which have fallen out of date and have now been superseded in the EU by the Network and Information Systems (NIS) 2 Directive.

As set out in the statement, the Bill will strengthen the UK's cyber defences and ensure that the critical infrastructure and digital services UK citizens and business rely on are secured. Cyber security is a critical enabler of economic growth, and by protecting our digital assets and ensuring the resilience of our critical services we are creating a stable environment that fosters innovation and attracts investment whilst protecting essential public services and infrastructure.

The Bill will:

- Expand the scope of regulations to protect more digital services and supply chains. The Bill will bring managed service providers that provide digital services into the scope of the regulatory framework.

- The Bill will allow regulators to designate a small number of high-impact suppliers to regulated entities as “Designated Critical Suppliers”. This will address vulnerabilities in the supply chain and reduce the threat of significant disruptions to critical services.

- Linked to the above measure, the bill will also amend the blanket exemption for small and micro-digital service providers (SMEs) allowing a small number of SMEs to be designated as critical suppliers and required to take appropriates security measures. This will reduce the risk that SMEs pose to essential services in a manner that minimises burdens to small businesses.

- Put regulators on a stronger footing. Regulators will be better equipped with the tools they need to perform their duties effectively, including improved cost recovery mechanisms and an expanded scope of what must be reported to a regulator during a cybersecurity incident.

- The Bill will update and enhance the current incident reporting requirements for regulated entities by expanding the incident reporting criteria, updating incident reporting times, streamlining reporting requirements by sharing information with regulators and the NCSC simultaneously, and enhancing transparency requirements for digital service providers and data centres.

- The Information Commissioner’s information gathering powers will be strengthened to improve its understanding of the landscape of cybersecurity threats.

- For regulated entities, the Bill will include a delegated power enabling Government to update existing security requirements. This would include a power to impose technical and methodological security requirements, including those relating to supply chain risk management, where appropriate and proportionate to do so and after consultation with stakeholders.

- The Bill will also allow the Government to update the regulatory framework in the future via secondary legislation, so that it can keep pace with an ever-changing cyber landscape. This will include updating the cyber security regulations to bring new sectors or sub-sectors into scope.

Department for
Science, Innovation
& Technology

In addition to the policy proposals outlined in the King's Speech for inclusion in the Bill, we have identified a number of **additional cyber security and resilience proposals**, as set out in the policy statement. The appropriate legislative vehicle for these has yet to be determined:

- Bring data centres into the scope of the regulatory framework, recognising their new status as critical national infrastructure and essential role in ensuring the stability and growth of our digital economy.

- Enable the Secretary of State to publish a statement of strategic priorities to establish a unified set of objectives and expectations for regulators.

- Provide new powers to the Secretary of State to direct a regulator, or regulated entities, to take action when it is necessary for national security. This will be invaluable in responding to the constant evolution of both the cyber landscape and the changes in tactics used by cyber threat actors.

I hope this supports your committee in engaging with the Bill's upcoming parliamentary process and your ability to scrutinise it.

Yours sincerely,

Feryal Clark MP
Parliamentary Under-Secretary of State for AI and Digital Government