City of London Corporation Committee Report

Committee(s): Digital Services Committee – For Information	**Dated:** 10/07/2025
Subject: Impact of the New Cyber Security and Resilience Policy Statement	**Public report:** For Information
This proposal: • **delivers Corporate Plan 2024-29 outcomes** • **provides statutory duties**	**Providing Excellent Services**
Does this proposal require extra revenue and/or capital spending?	No
If so, how much?	N/A
What is the source of Funding?	N/A
Has this Funding Source been agreed with the Chamberlain's Department?	N/A
Report of:	Chamberlains
Report author:	CJ Chapman

Summary

The purpose of this report is to inform about the recently published Cyber Security and Resilience Policy Statement Command Paper and to discuss its implications if any for the Corporation including the proposed actions needed to comply with the new policy.

This policy, presented to Parliament by the Secretary of State for Science, Innovation and Technology, outlines significant changes aimed at enhancing the UK's cyber security and resilience. Key points include the expansion of the regulatory scope to include Managed Service Providers (MSPs), strengthening supply chain security, empowering regulators, and ensuring the regulatory framework can adapt to emerging threats.

Recommendation(s)

Members are asked to:

- Note the report.

Main Report

Background

The government first announced it would be bringing a Cyber Security and Resilience Bill before parliament in July 2024. Hostile actors were increasingly exploiting the UKs dependence on online infrastructure, conducting cyber attacks that cause maximum disruption and destruction. Perhaps most notably the June 2024 cyber attack on Synnovis – which impacted critical health services in the UK demonstrating how fundamentally reliant our health services are on online technology.

In April 2025. The Cyber Security and Resilience Policy Statement Command Paper was presented to Parliament by the Secretary of State for Science, Innovation and Technology. The policy aims to enhance the UK's cyber security and resilience by expanding the regulatory framework, empowering regulators, and ensuring adaptability to emerging threats.

As such the Cyber Security and Resilience Bill is designed to strengthen the UK's cyber defences by enhancing the resilience of Critical National Infrastructure (CNI), essential services, and crucially - digital service providers. The Bill builds upon the existing Network and Information Systems (NIS) Regulations 2018 and introduces new regulatory powers, reporting duties, and oversight mechanisms for entities deemed vital to national security and economic stability.

Current Position

As a local council we provide and support essential services to the City of London. Although we are not formally designated as Operators of Essential Services (OES) and therefore do not currently comply to the NIS Regulations which this Bill builds upon.

The Bill targets specific sectors such as energy, transport, health, digital infrastructure, and data centres. These sectors are considered essential to the functioning of the nation and are regulated accordingly. In addition, the expanded scope of the Bill brings into the fold Relevant Digital Service Providers (RDSPs), or Critical Suppliers. Local councils have not been designated under these categories and we are therefore not subject to the regulatory duties imposed by the Bill.

Options

Although we are not in scope for this bill there are some actions we can take forward.

1. **Remain Vigilant to Changing legislation**
2. **Certify with NCSC Cyber Assessment Framework**

Proposals

1. **Remain Vigilant to Changing legislation** - The Bill acknowledges the rapidly evolving cyber threat landscape and the need for the UK's regulatory framework to remain agile and responsive. As the landscape adapts so must we. As legislation changes, we will be first in line to adoption and compliance.
2. **Certify with NCSC Cyber Assessment Framework -** The Bill proposes to formalise the use of the NCSC's Cyber Assessment Framework (CAF) as a benchmark for cyber resilience. The CAF provides structured guidance for assessing and improving cyber security across critical sectors. At the City of London we have already begun our journey to certification and have passed our initial independent assessment.

Key Data

- The policy brings more entities, including MSPs, into the NIS regulatory framework.
- The policy gives the government 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.

Conclusion

While the principles underpinning the Cyber Security and Resilience Bill—such as improved cyber resilience, incident reporting, and supply chain security—are relevant to all public sector bodies, the statutory provisions of the Bill do not currently extend to local government councils. Unless councils are explicitly designated in future secondary legislation, they remain outside the direct scope of the proposed regulatory framework.

By pursuing voluntary certification with frameworks such as the NCSC Cyber Assessment Framework, councils can benchmark their preparedness, identify vulnerabilities, and demonstrate a commitment to safeguarding vital services. Regularly reviewing internal processes, investing in staff training, and monitoring legislative changes will position the organisation to respond rapidly should regulatory obligations shift.

In conclusion, while local government remains outside the immediate remit of the Cyber Security and Resilience Bill, the fundamental message is clear: cyber security is a shared responsibility. By anticipating change, embracing best practices, and fostering a culture of continuous improvement, councils can play a pivotal role in protecting both their own operations and the wider communities they serve, ensuring ongoing trust and resilience in an increasingly digital world.

Appendices

- Appendix 1 - Cyber_Security_and_Resilience_Policy_Statement_Command_Paper

CJ Chapman
Information Security Manager
E: CJ.Chapman@cityoflondon.gov.uk