UK Parliament Calls on Cyber Specialists to Shape New Cyber Security Law

Submitted by: Zensec (Formerly SOLACE GLOBAL CYBER LTD)
Monday, 12 January 2026

The UK Parliament has formally invited cyber security professionals, organisations and subject-matter experts to contribute evidence to the Cyber Security and Resilience (Network and Information Systems) Bill, a major piece of legislation set to reshape the UK's cyber regulatory landscape.

The House of Commons Public Bill Committee has launched a call for written evidence, giving industry specialists a direct opportunity to influence how the Bill is scrutinised and potentially amended as it moves through Parliament.

The Bill is designed to update and expand the existing Network and Information Systems (NIS) Regulations, reflecting the growing scale, complexity and impact of cyber threats on the UK's economy and critical national infrastructure.

Key objectives of the legislation include:

* Expanding the scope of regulated organisations to cover areas such as managed service providers, data centres, critical suppliers and large load controllers

* Strengthening incident reporting requirements and regulatory oversight

* Enhancing enforcement powers, including higher penalties and regulator cost-recovery mechanisms

* Improving information-sharing arrangements and setting clearer strategic priorities for cyber regulators

These changes are intended to better protect essential services and digital supply chains from disruption, espionage and cyber attack.

The Public Bill Committee is explicitly seeking input from:

* Cyber security practitioners and specialists

* Technology and digital service providers

* Academics and researchers

* Organisations likely to be impacted by the Bill

* Industry bodies and professional associations

Written evidence submitted to the Committee will help inform line-by-line scrutiny of the Bill, ensuring that new obligations are practical, proportionate and effective in real-world environments.

This process gives cyber professionals a rare opportunity to shape legislation that will directly affect how cyber risk is managed, reported and regulated across the UK.

The Committee is expected to begin taking evidence from early February 2026, with scrutiny continuing into March. Submissions can be made now, and early engagement is encouraged, as the Committee may stop accepting evidence once its consideration of the Bill is complete.

Guidance on submitting written evidence is available via the UK Parliament website.

As cyber threats continue to escalate, regulatory frameworks must evolve alongside technology and attacker capability. Engagement from cyber professionals is essential to ensure that legislation:

* Reflects operational realities

* Supports effective incident response and cyber resilience

* Avoids unnecessary regulatory burden

* Strengthens trust across critical supply chains

The Cyber Security and Resilience Bill represents one of the most significant updates to UK cyber regulation in recent years — and industry voices will play a crucial role in shaping its final form.

Organisations that fall within — or may soon fall within — the scope of updated NIS regulations should act early to understand how these changes could affect their governance, incident reporting, risk management and supply chain obligations.

Zensec's cyber security specialists can help you:

* Understand upcoming regulatory expectations

* Prepare for enhanced cyber resilience and reporting requirements

* Navigate and respond to evolving cyber regulation with confidence

If you would like to discuss the implications of the Cyber Security and Resilience Bill, or need support preparing for regulatory change, contact the Zensec cyber security team today.

Distributed via Press Release Wire (https://pressreleases.responsesource.com/) on behalf of Zensec (Formerly SOLACE GLOBAL CYBER LTD)

Copyright © 1999-2026 ResponseSource, Northburgh House, 10 Northburgh Street, London, EC1V 0AT, UK

e: info@responsesource.com t: 020 3426 4051 f: 0345 370 7776 w: https://www.responsesource.com

responsesource