**CROWDSTRIKE RESPONSE TO THE UK CYBER SECURITY AND RESILIENCE (NETWORK AND INFORMATION SYSTEMS) BILL**

**6 February 2026**

## I. INTRODUCTION

In response to the UK Government's Cyber Security and Resilience (Network and Information Systems) Bill (the "Bill"), CrowdStrike offers the following views and recommendations.

We approach these questions from the standpoint of a leading international, AI-native, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

## II. COMMENTS

CrowdStrike welcomes the Bill's direction of travel to modernise the UK's NIS framework by strengthening oversight of systemic dependencies as well as explicitly recognising supply-chain compromise as a route to disrupt essential and digital services. This is well aligned to the threat landscape trends described in CrowdStrike's previous[1] and upcoming 2026 Global Threat Report (February 2026) and reflected in wider UK threat commentary - both are tracking increasingly professionalised cybercrime (including access brokers), growing exploitation of trusted third parties and supply chains, and disruptive ransomware activity targeting high-impact organisations. The broader coverage to be provided by a modernised NIS framework will help close known gaps and reduce systemic risk.

## III. RECOMMENDATIONS

### A. Mandate comprehensive endpoint and threat protection as a baseline capability (vendor-neutral, outcomes-led)

[1] *CrowdStrike 2025 Threat Hunting Report*, CrowdStrike, August 2025, https://www.crowdstrike.com/explore/2025-threat-hunt-report/crowdstrike-2025-threat-hunting-report?utm_medium=dir. Accessed 23 October 2025.

CrowdStrike recommends that statutory guidance and the Code of Practice explicitly treat modern endpoint and workload security as a baseline technical control for regulated entities—particularly those whose disruption would have significant societal or economic effects. The Bill currently describes technical controls at a high level; implementation should reflect that sophisticated UK-targeting threats increasingly exploit endpoints, identities, and cloud workloads as initial access and persistence layers.

A capability-based baseline should require regulated entities to deploy endpoint detection and response (EDR) capabilities that combine multiple layers of defence, including:

- behavioural analytics and detection,
- machine learning-based prevention,
- real-time threat intelligence, and
- automated response / containment workflows, to address threats such as ransomware, fileless malware, and zero-day exploitation.

An EDR solution with these capabilities allows defenders to perform threat hunting, incident response, and a variety of other essential cybersecurity tasks. EDR capabilities are a core pillar of most contemporary sophisticated security programs. This approach can remain technology-neutral (focused on outcomes and capability) while materially increasing the probability that regulated organisations can detect, contain, and recover from modern attacks.

**B. Align baseline controls to recognised frameworks ( NCSC CAF, ISO 27001) to reduce fragmentation**

CrowdStrike recommends that the Government use the Statement of Strategic Priorities and Code of Practice to drive clearer alignment with widely-adopted frameworks and standards. The Commons briefing explicitly recognises that strategic priorities could require regulators' guidance to reflect NCSC advice and even use the NCSC Cyber Assessment Framework as a basis for guidance. Implementation should also avoid creating "UK-only" technical compliance constructs that drive divergence from internationally accepted approaches without clear resilience benefit.

Accordingly, CrowdStrike recommends:

1. **Codifying multi-layered endpoint security as a baseline technical control** within the mapped expectations for NCSC CAF-aligned sector guidance, Cyber Essentials, and ISO 27001-aligned management systems; and
2. Ensuring the Code of Practice is written in a way that supports **outcome-based compliance** rather than static checklists, to maintain relevance as threats evolve.

As the UK Government is considering baseline controls, CrowdStrike recommends reviewing existing frameworks, such as Cyber Essentials Plus, to ensure it emphasizes modern, adaptive, and outcome driven cyber defence. Alignment across frameworks - and towards the goal of modern security practices - reduces compliance ambiguity for regulated entities, improves consistency across sectors, and helps regulators focus on measurable resilience outcomes.

**C. Recognise AI-driven and behavioural-based defences and ensure incident learning remains fit for modern systems**

CrowdStrike recommends that implementation of the CSRB—through secondary legislation, Codes of Practice and statutory guidance—explicitly recognises **AI-driven, behavioural-based and cloud-enabled security capabilities** as preferred approaches for safeguarding modern environments. Guidance should articulate these expectations in **capability terms**, prioritising solutions that can adapt to fast-changing threat activity and support **high-fidelity detection**, **predictive analytics**, and **automated containment/remediation**. This would help ensure the Bill's risk-management duties translate into "state of the art" security outcomes in environments where traditional perimeter assumptions no longer hold and where adversaries routinely exploit identity, endpoint and cloud control planes.

**D. Make incident reporting effective in practice: harmonise thresholds, reduce duplication, and standardise reporting formats**

CrowdStrike supports the Bill's objective of early national coordination via the UK NCSC. However, reporting timelines and content requirements should reflect the operational reality that the first hours of incident response are often characterised by uncertainty and rapidly changing facts. In addition, **overly ambitious early reporting expectations can risk diverting scarce responders away from containment and remediation, and can generate low-confidence or inaccurate reports**.

To maximise utility while minimising unintended burden, implementing regulations and guidance should adopt these design principles:

1. **Set objective materiality thresholds** (and sector examples) to prevent over-reporting and preserve signal-to-noise, noting the intention to capture incidents with significant actual or likely impact and the reliance on secondary legislation for detail.
2. **Explicitly recognise response prioritisation.** Guidance should acknowledge that organisations must prioritise containment and remediation in the critical initial phase; reporting must not impede stabilisation.

3. **Set a 72-hour notification timeline following international best practices.** To the extent that agencies develop requirements, we recommend they align to this timeframe.

While we believe strongly that time is of the essence in detecting and remediating cybersecurity incidents, we encourage policymakers and regulators to allow victim organizations a reasonable period of time to focus on response rather than reporting in the immediate wake of an incident. Reporting expectations should centre on a 72-hour window to enable higher-quality initial assessment and more reliable detail.

**E. Calibrate managed service provider and supply chain measures to reduce systemic risk without unintended harm**

We recognise critical supplier framework as a way to address supply chain concentration and "weak link" risk where disruption at the supplier level could have significant societal or economic impact.

However, CrowdStrike recommends caution with approaches that could inadvertently destabilise service delivery. For example, Committee-stage amendments propose a "critical risk threshold" concept for RMSPs, including duties to reduce customer numbers below a threshold and potentially terminate or vary contracts.

**We recommend** managing concentration risk through resilience and assurance outcomes rather than forced market-structure interventions. This could include:

- requirements for reasonable segmentation and least-privilege access across customers,
- stronger monitoring and rapid containment capabilities (including endpoint/workload visibility),
- incident response and recovery playbooks, and
- demonstrable security governance and testing.

This better supports continuity of essential services while still reducing systemic exposure.

## IV. CONCLUSION

CrowdStrike supports the Bill's core objectives—modernising the UK's cyber regulatory environment, strengthening incident reporting, addressing systemic supply chain risk, and enabling greater regulatory consistency and capability.

CrowdStrike would welcome further engagement with DSIT, regulators, and Parliament to discuss the recommendations above, particularly the strategic opportunity to make modern, AI-enabled endpoint and threat protection a baseline expectation for regulated entities—implemented in a technology-neutral, outcomes-led way through guidance, codes of practice, and aligned frameworks.

## V. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/.

## VI. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

**Drew Bagley**
VP & Counsel, Privacy and Cyber Policy

**Līga Rozentāle, CISM**
Director, Public Policy EU/International

Email: policy@crowdstrike.com

CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.

###