ONLINE SAFETY ACT NETWORK

Written evidence to Cyber Security and Resilience Bill Committee

---

About the Network

1. The Online Safety Act Network brings together over 70 civil society organisations, campaigners, academics and advocates with an interest in the implementation of the Online Safety Act 2023 (OSA). More details about our work are here[1]. The Network continues the work carried out by Professor Lorna Woods OBE, William Perrin OBE and Maeve Walsh at Carnegie UK[2] during the passage of the Online Safety Bill: Professor Woods' proposal for a "duty of care" to address online harm reduction formed the basis of the OSA; and the Carnegie team supported Members, Peers and Select Committees during the Bill's passage, gave evidence to Parliamentary inquiries and Bill Committees and were acknowledged by Parliamentarians in both Houses for their contribution.

Summary

2. This evidence submission puts the case for a greater focus on "security by design" in the Cyber Security and Resilience (CSR) Bill, which - if not rectified - is a potentially missed opportunity for the Government to embed the principles of "by design" in this updated regulatory framework and provide alignment with the overarching objectives of the Online Safety Act.

Background

3. The objective of the CSR Bill to update the NIS regulations is welcome. The NIS regulations, are proportionate, risk-based requirements, focused on the architecture and operations of the systems that underpin the UK's digital networks and information systems. They put the responsibility on in-scope services to "take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies."

4. The CSR Bill repeats this language - for example, at 14B ("An RMSP must identify and take appropriate and proportionate measures to manage the risks posed to the security of network

[1] https://www.onlinesafetyact.net/
[2] https://carnegieuk.org/programmes/online-harms/

and information systems on which it relies for the purpose of providing managed services within the United Kingdom")

5. The language in both the NIS Regulations and the CSR Bill reflects what one might call a "by design" approach to security and resilience: that a service should seek first to reduce the risk of harm before seeking to manage it and that, informed by a risk assessment, measures should be taken across all elements of the system/service throughout the lifecycle of the system/service and its operation - in design, deployment, management and retirement.

6. In recent years, the Government has increasingly been promoting the importance of a "by design" approach to both cyber security and online safety, but the legislative and regulatory frameworks to embed this as an obligation on regulated services are lagging behind. The Online Safety Act (OSA) has a requirement in its very first section[3] that services regulated by the Act must be "safe by design" but - as we describe here[4] - this has not been followed through by Ofcom in the codes, guidance and other supporting documentation to operationalise the Act. We suggest proposals to address this below.

7. Conversely, despite there being significantly more supporting material on "security by design" produced by the Government and the National Cyber Security Centre which sets out how to operationalise this principle, there is no mention of "security by design" in the CSR.

8. As far back as 2019, the Government's National Cyber Security Centre published a set of design principles for Cyber Security[5], as follows:

    1. **Establish the context before designing a system**
    Before you can create a secure system design, you need to have a good understanding of the fundamentals and take action to address any identified short-comings.
    2. Make compromise difficult
    Designing with security in mind means applying concepts and using techniques which make it harder for attackers to compromise your data or systems.
    3. Make disruption difficult
    When high-value or critical services rely on technology for delivery, it becomes essential that the technology is always available. In these cases the acceptable percentage of 'down time' can be effectively zero.
    4. Make compromise detection easier
    Even if you take all available precautions, there's still a chance your system will be compromised by a new or unknown attack. To give yourself the best chance of spotting these attacks, you should be well positioned to detect compromise.
    5. Reduce the impact of compromise
    Design to naturally minimise the severity of any compromise.

[3] https://www.legislation.gov.uk/ukpga/2023/50/section/1/enacted
[4] https://www.onlinesafetyact.net/analysis/safety-by-design/
[5] https://www.ncsc.gov.uk/collection/cyber-security-design-principles

9. In October last year (2025), the Government Security Group launched its "secure by design" framework[6] which aims to improve its own "cyber resilience" and "improve data-sharing between organisations". It was developed with the NCSC and industry experts and is supported by extensive documentation, including a set of 10 principles for security by design, a policy statement, implementation manuals, guidance and toolkits. It is a core requirement of the Government's "Cyber Security Standard".

10. Given that these detailed frameworks exist - and are widely understood and adopted within the industry - there is an opportunity with this Bill for the Government to take inspiration from the Online Safety Act by introducing a simple amendment at the front of the Bill to mirror the first section of the OSA and make clear the services in scope are required to be "secure by design". This would then enable a definition of "secure by design" to be included in the Bill and for a subsequent codes of practice - for which the BIll makes provision - to further set out the "by design" requirements. This would help operationalise these requirements and would neatly fit with the Bill's provisions for that code to relate to the "identification, management and reduction of risks of security and operational compromises".

11. The Statement of Strategic Priorities[7] that will flow from the CSR Bill would then also provide further opportunity to dovetail the security and safety objectives. The Government in its supporting documentation for this Bill has said the objectives within a statement of strategic priorities "could relate to the way in which regulators' guidance reflects National Cyber Security Centre (NCSC) advice, or could seek to ensure that different sectors have contingency plans in place to increase security at times of heightened threat. Overall, the objectives and priorities set are expected to support delivery of the UK's national cyber strategy."

12. For the services which are regulated by the NIS regulations, this Bill and the Online Safety Act - number-based interpersonal services, search engines, cloud storage sites which host file-sharing services and can describe social media services too - this would provide a consistent, complementary approach. Security by design within this context is the same as safety by design with the online safety context: a requirement that those responsible for developing the services on which we all depend do so in a way that avoids risk of harm.

Recommendation

13. **We suggest that the CSR is amended to include a simple clause at the front of the Bill to mirror that from the OSA: that the purpose of the Bill is for regulated services to ensure they are "secure by design". We then propose a definition of "security by design", drawn from well established frameworks in other industrial sectors, to provide clarity and structure for the**

[6] https://www.security.gov.uk/policy-and-guidance/secure-by-design/about/

[7] https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets/statement-of-strategic-priorities

regulatory regime and within which the existing guidance and principles can be embedded. This then also allows for the production of a "security by design" code of practice and its inclusion in the subsequent Statement of Strategic Priorities.

Safety by design in the OSA

14. We mentioned above that the objective in the OSA to ensure regulated services are "safe by design" has not been fully implemented. This is despite the then Government, in 2021, setting out some clear principles for "safety by design"[8] for social media services and, in May 2025, the former DSIT Secretary of State making "safety by design" his first priority in his Statement of Strategic Priorities. Indeed, "safety by design" is not mentioned in Ofcom's proposed Plan of Work for 2026/27 (see our response to their consultation here), nor was there any update on specific work relating to safety by design in their 2025 Progress Report on implementing the OSA.

15. The introduction of the requirement that products be safe by design in s1 OSA was significant but there are, however, a number of possible interpretations of the phrase. To ensure clarity, effectiveness and cross legislative coherence, the OSA should also be amended to include "by design" principles to match those proposed to underpin security by design in the CSR.

16. As part of our 10-point Plan for strengthening the Online Safety Act, we are calling for the Government to address this by amending the OSA to provide a clear definition of "safety by design" and requiring Ofcom to produce a code of practice.

Recommendation

17. **If the Government is serious about delivering on Parliament's intent that one of the OSA's primary objectives is to make services "safe by design" and agrees with the repeated concerns - raised by Parliamentarians across both Houses as well as civil society experts - about Ofcom's weak and cautious implementation of the regime, it could use the CSR to amend the OSA to strengthen its "by design" focus. We provide amendments to insert a definition of "safety by design" into the OSA and introduce a code of practice at the end of this briefing.**

Online Safety Act Network
February 2026

[8] https://www.gov.uk/guidance/principles-of-safer-online-platform-design

ANNEX: proposed CSR amendments

INSERT AFTER CL 2

Security and Resilience by Design

2A

(1) Duties imposed by this Act, and by the NIS regulations, seek to ensure (among other things) that services regulated by this act and the NIS Regulations are secure by design

(2) Where services take steps or measures to manage risk to the security of their services through technical measures as required by this Act or the NIS Regulations, they should follow the following principles:

(a) security of design hierarchy of risk control principles, as follows:

(i) avoid introducing security risks where possible;

ii) evaluate security risks that cannot be avoided and take appropriate measures to mitigate or to manage risks;

(iii) remediate where necessary

(b) ensure security and resilience is taken into account through the entire lifecycle of the service and the functionalities making up the service, including the following stages: design, development, deployment, management, and retirement

(c) consider safety across all features of the system; combat security risks as close to source as possible.

Explanatory note: the first part of this amendment mirrors the formulation that was inserted at the front of the Online Safety Act (s1) re ensuring that services regulated by the Act are "safe by design"

The amendment then suggests a definition of what "security by design" means in this context, structured around a hierarchy of risk control principles, which are drawn from well established principles from other industrial sectors.

INSERT AFTER CLAUSE 60

Insert in the Online Safety Act after Section 4

4A
(1) For the purposes of this Act for safe by design means that the following principles have been followed in the development and deployment of the service and its features and functionalities:

(a) security of design hierarchy of risk control principles, as follows:

(i) avoid introducing risks of harm arising where possible based on, inter alia, product testing;

ii) evaluate risks of harm that cannot be avoided and take appropriate measures to mitigate or to manage risks;

(iii) remediate where necessary

(b) ensure risk of harm is taken into account through the entire lifecycle of the service and the functionalities making up the service, including the following stages: design, development, deployment, management, and retirement

(c) consider risk of harm across all features of system; combat risks as close to source as possible.

Amend s 41 Online Safety Act

Insert new s41(4A)

OFCOM must prepare and issue a code of practice for providers of Part 3 services on safety by design in accordance with s 1(4) for the purpose of compliance with relevant duties

Note: This is already defined at s 41(10)

Explanatory note: This amendment would amend the OSA to ensure a complementary definition of "safety by design" (currently lacking in that Act) so that - consequent to the proposed amendment to clause 2 - the "by design" frameworks in both sets of legislation are comparable.

It also amends the OSA to require Ofcom to produce a code of practice on safety by design.