**National Cyber Security Strategy 2019-2024**

**Mid-Term Review, Consultation**

**Submission by Amazon Web Services (AWS)**

**31 January 2023**

## Executive Summary

Conditions have changed significantly since the National Cyber Security Strategy 2019-2024 ("the Strategy") was first published. Cybercrime has become an even bigger threat than before. Government, meanwhile, has transformed its approach to technology use, most notably through its direction that public sector bodies (PSBs) move to the cloud in order to both strengthen cybersecurity and achieve other goals. The Strategy and the National Cyber Security Centre (NCSC) can now pivot and help PSBs move more rapidly to the cloud so that they can both improve their cybercrime defences while simultaneously delivering on Government policy. For the NCSC to deliver on that work programme, it should be resourced more strongly and encouraged to continue its strong collaboration with industry. The NCSC should also both provide new cloud security guidance to PSBs and provide a separate direction that makes clear the cybersecurity advantages of cloud technology.

## Cybersecurity and policy environment & appropriate NCSC response

The global cyber threat environment, as well as the Irish Government's domestic approach to technology, have both changed considerably since the Strategy was originally published in 2019. We respectfully submit that these respective shifts require a commensurate response from the NCSC, the details of which are set out further below.

The global cyber threat situation has, as the Consultation Paper recognises, deteriorated since 2019. This is partly due to the inexorable shift to digital in daily life – fuelled by increased connectivity, ever-increasing use of the internet, and the shift to remote- and hybrid-working arrangements – has accelerated further, attracting the unwanted attention of greater numbers of cybercriminals. This in turn has led to more cybercrime in all its forms (e.g. malware, phishing, ransomware). Ireland, including its public sector, has not been immune from this trend. The ransomware attack on the Health Service Executive (HSE) in 2021 is the most notable example of that. The Irish public sector could be targeted further by cybercriminals in the future. Russia's invasion of Ukraine is another exacerbating factor, in that global political instability can be a fertile climate for cybercrime.

On the domestic policy level, the Irish Government's approach to technology use has been transformed since 2019. Government now has a new bold and ambitious vision for how it will use technology to deliver better public services. That vision is set out in both the public sector ICT strategy ("Connecting Government 2030") and the national digital strategy ("Harnessing Digital"), which were published in 2022. Those strategies are built around a number of headline goals, including having 90% of applicable public services consumed online by 2030, 20% of employees in the public sector working remotely, and 75% enterprise take up of cloud computing by 2030.

At the heart of both strategies is Government's commitment to moving rapidly to the cloud, in order to enable its digital goals. Connecting Government 2030, for example, commits Government to henceforth taking a cloud-first approach to delivery of services, both public facing and back office. Government Ministers have been vocal too about the importance of cloud adoption, particularly as a means to strengthen cybersecurity. The Minister for Finance, Michael McGrath, for example, has said[1] that "Organisations should no longer decide whether to move to cloud for new or existing systems. The decision to be made now is what, how and when to move to cloud, which can offer a step change in carbon efficiency, **security** [*emphasis added*], and value for money." The Minister of State for eGovernment, Ossian Smyth, meanwhile, has described[2] cloud computing as "underpinning Government's ambitions [in the digital transformation of public services] by providing a cost-effective and **resilient** [*emphasis added*] way to avail of ICT infrastructure". This strategic political commitment to cloud use is now being matched by efforts to ensure that PSBs can more easily procure the technology. The Office of Government Procurement is currently working towards the establishment of Ireland's first ever cloud procurement framework, which it has committed to launching in Q4 2023.

It is therefore clear that Government sees wide-scale cloud adoption as integral to delivering on its vision for digitalisation and strengthened cybersecurity. The well-documented security benefits of the cloud, as referenced above, have been cited repeatedly. The HSE cyberattack also underlined the security advantages that the cloud provides. The independent report by PwC on the circumstances of that attack, which was commissioned by the HSE, found that cloud-based systems were largely unaffected by it. It follows that the damage wreaked by cybercriminals would have been less severe had the HSE's systems been architected using the cloud. The findings of the report thereby underline the importance of delivering on the Government's cloud ambitions in order to strengthen the public sector's cybersecurity defences.

We respectfully submit that the NCSC now has a critical role, both in reviewing its 2019-2024 strategy but also more generally, in enabling the transition to cloud so as to enhance cybersecurity. The NCSC can help achieve two inter-connected goals in this context. First, accelerating cloud usage by PSBs as an effective response to the deteriorating global cybersecurity situation. And secondly, helping Government deliver on its own cloud goals, which are substantially driven by cybersecurity considerations.

For the NCSC to be able to deliver on these objectives, we recommend that a number of steps be taken.

[1] https://www.oireachtas.ie/en/debates/question/2021-03-04/51/

[2] https://www.gov.ie/en/press-release/e1b38-minister-mcgrath-and-minister-of-state-smyth-launch-guidance-to-support-public-procurement-of-cloud-computing-services/

### (i) Resourcing of the NCSC

Despite recent budgetary increases, the NCSC remains under-resourced. Its budget is dwarfed by the budgets of comparable cybersecurity authorities in other EU member States. The NCSC's financial allocation has not kept pace either with the growth of Ireland's tech sector over the last decade (estimated at 12% annually since 2013). The NCSC therefore requires further funding so that it can access the technological tools and human resources necessary to better protect PSBs, and Ireland more generally, from cybercrime.

As Ireland is a recognised global hub for technology firms, it should also benefit from a world-leading national cybersecurity authority befitting of that international standing. The NCSC has already developed a strong reputation. Further resources, however, would allow it to become a genuine thought-leader and, more importantly, enhance its capacity to deliver its core cybersecurity functions.

### (ii) Collaborating with industry

There are few areas where public sector-private sector collaboration is as important as cybersecurity. Both sectors have much to offer to one another in their efforts to combat the scourge of cybercrime.

AWS has long been focused on working directly with cybersecurity agencies around the globe. We want to support their work and lend our expertise and experience, where helpful. That is also the case with the NCSC. We have already successfully worked in collaboration with it in the context of the AWS Global Cyber Security Programme (GCSP). We hope this project has helped support the overall mission of the NCSC and we aim to strengthen it further in future. We commend the NCSC for its constructive approach to industry engagement and we suggest that this continue so it can continue to scale its capabilities.

We welcome the Consultation's reference to the establishment of a Strategic Advisory Group of Cybersecurity Research Stakeholders. AWS would be happy to work in conjunction with the NCSC on this working group, once established.

### (iii) Cloud security guidance

Irish PSBs are increasingly seeking to move to the cloud on cybersecurity grounds, both on their own accord but also in response to overarching Government strategy and direction. Guidance from the NCSC to PSBs – building on the NCSC's useful "Public Sector Cyber Security Baseline Standards" publication – on how they can maximise the considerable cybersecurity benefits of the cloud would be helpful. PSBs, understandably, do not always have the comprehensive in-house experience that they need for this process. Further NCSC guidance would therefore help ensure the transition to the cloud will be as seamless as possible and that PSBs will fully benefit from its considerable cybersecurity advantages. It could also assist PSBs in leveraging Sensor, the NCSC's threat detection programme, in a cloud environment. The UK National Cybersecurity Centre already provides excellent such cloud security guidance to UK PSBs. This provides a convenient template from which the NCSC could draw in devising a similar publication for Irish PSBs. AWS stands ready as well to support this process.

### (iv) NCSC direction on cloud adoption as key to enhancing cybersecurity

The Government has already made its position on cloud adoption clear, as referenced above. A complementary written direction by the NCSC to PSBs, that would direct that cloud adoption must be pursued in order to enhance cybersecurity defences, would help deliver on Government's policy.

**Point of Contact:**

[redacted]
Head of Public Policy, Ireland
[redacted]