Workday Comments on the Government of Ireland's National Cyber Security Strategy 2019-2024 Mid-Term Review Consultation

1 February 2023

Workday appreciates the opportunity to submit comments to the Department of the Environment, Climate and Communications' consultation on the National Cyber Security Strategy review.

Workday is a leading provider of enterprise cloud software. Our software-as-a-service (SaaS) products for financial management, human resources, planning, spend management, and analytics have been adopted by thousands of organisations around the world - from medium-sized businesses to more than 50 percent of the Fortune 500. In Ireland, Workday has 1800 employees with more than 70% of the Irish site engaged in Product & Technology software development engineering roles. In April 2022, Workday announced its plans to develop its new 55,000 sqm. EMEA HQ on the Grangegorman campus.

Workday's top priority is security. We know safeguarding our customers' most precious assets - people and financial data - is a tremendous responsibility. That's why we infuse security into everything we do, we employ rigorous security measures at the organisational, architectural and operational levels to ensure that our customers' data, applications and infrastructure remains safe.

Workday welcomes the Government's priority to take stock of progress made in delivering the 2019 Strategy, and to identify possible measures for the remaining years. In addition, we are pleased the Government is consulting and collaborating with relevant stakeholders during this process and as such, offer the following feedback.

Critical National Infrastructure Protection

Workday is pleased the Government prioritises the protection of Critical National Infrastructure through the continued application of the NIS Directive, while also acknowledging the overhaul that the NIS2 will bring to the Single Market and the significant preparatory work that will be needed by Government and industry in advance of the deadline for transposition on 17 October 2024 and its application on 18 October 2024. Workday also takes note of the implementing acts that still need to be developed by the European Commission for certain service providers in scope including cloud, data centre and managed services, and which will help ensure consistency across EU Member States.

Beyond the NIS2, Workday also would like to highlight the EU cybersecurity rules for the financial sector and their ICT third-party service providers (DORA), which will also bring important impacts to the sector. It is critical for the NIS2 to be fully aligned with DORA and other cybersecurity legislation such as the Cybersecurity Act, to ensure legal certainty for impacted companies.

We are pleased to see the Government is already taking steps to prepare for NIS2, for example updating risk assessments on the vulnerability of all Critical National Infrastructure and services to cyber-attack, and creating a database of critical infrastructure, vendors and managed services. We recommend the

Government consult and collaborate with impacted entities early on and throughout this process, as well as across government departments to ensure a seamless transition from existing to future cybersecurity frameworks and measures.

Adequate resourcing of the National Cyber Security Centre of Ireland (NCSC) will be important to enable effective leadership and expertise of future EU-level cooperation groups under NIS2 such as the Cooperation Group, CSIRTs Network and EU-CyCLONe. Government should also ensure Ireland is well represented in other EU-level groups such as the European Cybersecurity Competence Centre and Network of National Coordination Centres. Their remit to support innovation, maintain excellence in standards and reinforce EU cyber competitiveness will be valuable in the context of growing the sector in Ireland.

Cyber Security for the Public Sector

Workday supports governments and businesses with their digital transformation by leveraging the benefits of cloud services, providing flexibility, increased productivity, enabling efficiencies and improving security. As mentioned above, security is top of mind for Workday and we deliver security across all aspects of our service including ensuring regulatory compliance e.g. GDPR and obtaining certifications e.g. ISO 27001, 27017 and 27018, as well as data security measures including physical security, encryption of data at rest and in transit, data backups, disaster recovery and authentication etc.

Despite the benefits of cloud security and actions taken by Workday to incorporate security into everything we do, we are concerned by a growing trend by some governments in Europe to consider or enact laws and policies with data localisation and extraterritorial immunity requirements. These requirements would in effect exclude non-EU companies from participating in certain public procurement tenders and industry sectors and dramatically limit European governments' and companies' ability to select the cloud service provider that best meets their operational needs with state-of-the-art cyber protections. This could have the unintended consequences of weakening, rather than improving the level of security required of Government cloud computing service providers. If such measures were to expand across the EU, including through the EU cybersecurity certification scheme for cloud services (EUCS), the cost of compliance and oversight could increase significantly without improving security outcomes for both public and private sectors.

For this reason, we urge the Government to avoid adopting such sovereignty measures and to consult with industry as it plans to issue recommendations on the procurement of software, hardware and cloud computing services on Government IT in Q1 2023, and in its review and update of the Baseline Security Standards by Q4 2023.

In addition, we welcome that the Baseline Security Standards are based on NIST, European and international standards and encourage their update in Q4 2023 to continue to do so. Internationally recognised standards leverage global security expertise from governments, industry and academia, enabling international interoperability, innovation and less cost than national or local standards.

Skills

The challenge faced by governments and industry in attracting and retaining employees with cyber expertise is well known. One of the challenges is not only to simply identify the skills that are needed, but also to help existing workers identify both the skills they currently have and those that would grow their careers. Such a skills-based approach widens the talent pool and finds workers with skills that would thrive in the dynamic environment that cybersecurity requires.

At Workday, we believe that understanding an employee's skills is essential and an imperative to the future of work. That is why we have introduced Workday Skills Cloud, which leverages a skills ontology, or a way of understanding what makes up a skill and the relationships between different skills. Skills Cloud was developed using machine learning to process massive amounts of data associated with job roles and responsibilities; it enables job seekers and workers to better describe the skills they already have, receive suggestions about roles suited to their skills and understand which skills to acquire for career growth and continued learning.

Skills are the currency of the changing world of work, and a focus on skills offers the right framework for approaching today's pressing workforce development challenges. By looking at skills over pedigree, the Government can make smarter hiring decisions, including from a pool of trainees, for employees wishing to make a change to their career path, and to enrich the career journeys of cybersecurity professionals with informed upskilling and greater internal mobility.

Another area of skills focus for Workday is our partnership with Technological University Dublin (TUD). Workday signed a partnership with TUD in April 2022. This involves a number of key engagements including education outreach, workforce development and next generation research. We have co-developed a modular programme with TUD to upskill Product and Technology employees in key cyber security areas. This accredited security training will incentivise developers and engineers to become Security Champions in support of the global security programme while also fostering security as a strategic capability within Workday Dublin. This investment will allow the company to build a Security Centre of Excellence in Dublin. The Security Continuous Professional Development (CPD) training will focus on one primary module with the option for students to achieve a MSc In Applied Cyber Security from TUD.

Enterprise development and engagement

Workday welcomes the Government's efforts to collaborate and engage with industry including via Cyber Ireland. Workday is a member of Cyber Ireland and supports its mission to advance the sector with specific focus on skills and research. With over 7,000 people employed in cyber security, it is important that Ireland continues to nurture and develop the domestic talent to fuel growth in this important space. This competency supports a number of strategic high value business functions and ultimately opens up significant growth opportunities across organisations.

We support the work that Cyber Ireland has carried out in recent months including the policy recommendations outlined in the paper 'Achieving Our Cyber Potential 2030'. We also support proposed further measures identified in the consultation, such as to develop a strategy on the cyber industry in

Ireland, improve industry engagement between Ireland and other EU Member States and address the cyber skills challenge, including the lack of diversity in cybersecurity. The Cyber Security Skills Report 2021 was useful to understand more about the skills shortages and future talent pipeline needs. It would be valuable to understand how the Government is responding to these findings. These are all important actions that Workday looks forward to supporting through our participation in Cyber Ireland and directly with the Government in 2023.

In addition to Workday's support for Government's engagement with industry, we also welcome the efforts Government has taken to strengthen its engagement internally across departments, with like-minded third countries and international organisations. Cybersecurity threats do not respect a country's borders and cybersecurity policies must be taken in cooperation with and alignment to Ireland, the EU, and with like-minded countries such as the United Kingdom and the United States.

At international level, we welcome the establishment of a further permanent attaché at the Embassy of Ireland to the United States in Washington DC to ensure regular dialogue and coordination on cybersecurity trends, threats, and policy responses across the Atlantic.

Workday appreciates the opportunity to provide this feedback to DECC. We look forward to the process moving forward including upcoming webinars and continued progress on existing measures and further measures to realise the 2019 Strategy and lay the groundwork for the future strategy post-2024. Please contact [redacted] and [redacted], for further information and to answer any questions you may have.