CYBERSKILLS
Building Ireland's cyber security skills

[redacted]

National Cyber Security Strategy MTR Consultation
Cyber Security and Internet Policy Division
Department of the Environment, Climate and Communications
29-31 Adelaide Road
Dublin

24th January 2023

To Whom it may concern:

On behalf of the Higher Education Authority (HEA) Human Capital Initiative (HCI) Pillar 3 funded initiative Cyber Skills (www.cyberskills.ie) Institute Executive Team (IE-Team) please find attached our stakeholder feedback on Ireland's National Cyber Security Strategy Mid Term review.

Please note the following legend was used to categorise the feedback provided:
R – Recommendation to update the text
F – Formatting recommendation
FM – Recommendation for a Future Measure
U – Measure No – Proposed update to an existing measure
P – Measure No – Defined progress against an existing measure that should be recorded

The Cyber Skills team if required is available to discuss any of the feedback provided below or participate in further stakeholder engagement on the NCSC Cybersecurity Policy.

Further information on the Cyber Skills initiative is available via the following links:
Cyber Skills General Websitez– www.cyberskills.ie
Cyber Skills and Cyber Ireland SFI Discover Funded Project Cyber Futures – www.cyberfutures.ie
Cyber Skills Cyber Range Infrastructure – range.cyberskills.ie
Cyber Skills led Ireland's Check My Link Service – check.cyberskills.ie

Regards,

[redacted]
(on behalf of Cyber Skills IE Team)

CYBERSKILLS
Building Ireland's cyber security skills

Summary of Cyber Skills feedback

No	Section Name	Legend	Stakeholder Feedback
2	Vision	R - Protect	**Update in text** The vision statement needs to reflect a move from readiness to resilience in the protect statement i.e. move from just protect to protect/prevent, withstand and recover.
		F	**Formatting Recommendation** This section should be reorganised that identify key national and EU policy in separate sub (sub) sections. At present the only national policy referred to is the Harnessing Digital policy.
		R	**Update in text** The NCSC Capacity Review is not a policy development and should be moved to Section 6 under National Capacity Development, progress to date.
		R	**Update in text** Key Irish policy referring to security and privacy not included in the current document: • Enterprise 2025 Renewed, "The pervasiveness of technological advances requires a new way of thinking for enterprise policy if we are to capitalise on opportunity and ensure that no person is left behind. The policy agenda is broad, including progressing the Digital Single Market, data protection and data security, intellectual property regime, investments in digital infrastructures, up-skilling and re-skilling people in the workforce, the education and training systems, employment legislation and digital taxation." • Ireland's Industry 4.0 Strategy, "Framework conditions are a critical part of the business environment for Industry 4.0, supporting established firms and start-ups and attracting new Industry 4.0 investment to Ireland. Given the pervasiveness of the digital transformation across our economy and society there are a broad range of framework conditions that need to be in place to support an inclusive and sustainable transition. These include, for example, connectivity, trust and security, data privacy and digital literacy." • Project Ireland 2040, "Ireland is very attractive in terms of international digital connectivity, climatic factors and current and future renewable energy sources for the development of international digital infrastructures, such as data centres."

5.4	EU Cyber Security strategy for the digital decade	R	You should cite relevant EU documents to refer the user properly. • EU 2018, ***A Europe that protects: Countering hybrid threats*** https://www.dsn.gob.es/sites/dsn/files/hybrid_threats_en_final.pdf • European Policy Centre 2019, ***Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox*** https://www.epc.eu/content/PDF/2019/pub_9081_responding_cyberattacks.pdf • European Union Institute for Security Studies 2017, ***The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?*** https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sa nctions.pdf • Council of European Union 2017, ***Cyber Diplomacy Toolbox*** https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf
		R	**Update in text** In the EU Cyber Diplomacy and the Strategic Compass section you are missing a reference to how the EU intend to boost cyber defence capabilities through the Cyber Defence Policy Framework (CDPF).
		R	Resilience of Critical Entities directive missing - You are missing reference to the directive on the resilience of critical entities (CER Directive) which replaces the Critical Infrastructure Directive on 2008. https://digital-strategy.ec.europa.eu/en/news/new-stronger-rules-start-apply-cyber-and-physical-resilience-critical-entities-and-networks?pk_source=ec_newsroom&pk_medium=email&pk_campaign=Shaping%20Europe%27s%20Digital%20Future%20website%20updates
		R	**Update in text** DORA is missing and is a key legislation that should be included.
7	Critical National Infra Protection	U - M3	**Update Measure** Measure 3 needs to be updated to NIS 2.
6	National Capacity Development	FM	**Proposal for future Measure** Ensure that adequate cybersecurity is built into our evolving critical national infrastructures for energy, water, transport,

			communications and health. Taking the example of green energy, Ireland has the potential to become a renewable energy exporter to Europe but this will demand a strongly-digitalised national energy management system that will become a target for international criminal activity and cyber-espionage: it will have to be cybersecure.
9	Skills	U - M12	**Update Measure** This measure should be updated to include other government funded initiatives such as the HEA HCI P3 initiative Cyber Skills. This initiative represents an investment of 8.1M EUR by the government in responding to industry needs on the topic of cyber security skills.
		U – M13	**Update Measure** The measure as it currently stands references SFI and its smart futures programme. Reference to this specific programme by SFI is too restrictive. The measure should be updated to say something along the line: Develop cyber security awareness programmes/initiatives that focus on improved cyber resilience and awareness among citizens of all ages for improved cyber hygiene and promotion of cyber security careers.
		U – M14	**Update measure** Measure 14 there has not been any significant investment made in cybersecurity research. To propose a revision to measure 14: Science Foundation Ireland(SFI)/Higher Education Authority (HEA)/Enterprise Ireland (EI), will make cybersecurity a strategic research priority by explicitly listing it as a thematic area in future co-centre/centre/north south research partnerships/programmes.
		FM	**Proposal for new measure** There is a global shortage of cybersecurity professionals but qualification typically requires a undergraduate computing degree and postgraduate specialisation. We need to deliver highly skilled graduates to the sector at a faster rate by investing in cybersecurity education and training at all NFQ levels. We need to achieve this goal in a way that does not compromise on the quality of education. In order to achieve this we need to establish a baseline in cybersecurity education and agree key knowledge/skills/abilities that courses should teach. These baseline standards already exists i.e. NIST NICE and UK NCSC baseline standard. ENISA recommends that 50% of cybersecurity courses should be dedicated to practical activities. This should be enforced through the established baseline standard in cybersecurity education.

		FM	**Proposal for new measure** Invest in initiatives/academic programmes that focus on collaboration in the HEI sector. This is required as cybersecurity as a discipline is constantly evolving and training/education needs to adapt at a faster rate. As a result curricula is struggling to keep up, mainly because HEI providers work in silos and lack mechanisms to quickly incorporate material on emerging threats or new skills.
		FM	**Proposal for future Measure** A fixed % of all national funding for Digitalisation to be specifically ringfenced for cybersecurity.
		FM	**Proposal for future Measure** Track research spend on cybersecurity by developing standard classification system for public expenditure for research in Ireland.
		FM	**Proposal for future Measure** Develop a national cybersecurity infrastructure to support collaborative R&D and skills/training. This infrastructure can also be used to test the cyber resilience of national critical infrastructure and response to cyber attacks. **Progress to date in this infrastructure** Munster Technological University (MTU) in collaboration with University of Limerick (UL) and Technological University Dublin (TU-Dublin) have designed/procured and implemented a cyber range infrastructure. It has achieved this by securing funding (approx €2M from SFI CONFIRM, EI, HEA and Technological University Transformation Fund) and led the design/procurement/implementation of a cyber-range infrastructure enabling advanced R&D, skills and training. This unique national infrastructure, accessible through SFI CONFIRM, MTU, UL and TU Dublin supports the full spectrum of cybersecurity research across all TRL levels and skills/training at all NFQ levels. Expansion of this infrastructure is required to make it available a national asset.
		FM	**Proposal for future Measure** Understand and respond to the barriers that reduce diversity & inclusion, and exclude learners from disadvantaged communities from participating in the cybersecurity industry. We should aim to achieve this by conduct a national diversity & inclusion survey, understanding and benchmarking and track levels of diversity and inclusion in the industry. UK NCSC undertook a study of this natursece with the aim of "catalysing organisations to challenge their assumptions and take evidence based actions". See the below report for template:

			https://www.ncsc.gov.uk/report/diversity-and-inclusion-in-cyber-security-report
		P – M13	**Progress to Date** Cyber Skills and Cyber Ireland secured funded for an SFI Discover funded project focused on building cyber-resilient citizens through more effective cyber-hygiene practices, training, and awareness. As part of this programme it has made the following impact/progress: • Promotion of cybersecurity careers/improved cyber hygiene practices for secondary school students (age 16-19) through our cyber-academy which is a week-long immersive programme teaching key cybersecurity skills (https://cyberskills.ie/explore/events/cyber-security-academy.html). • Development of cyber career videos which are regularly posted and updated online to promote cybersecurity careers (https://cyberfutures.ie/careerstories/) • SmartEDU Club – 2 day cybersecurity workshop to engage young people and adults in creating secret messages, solving riddles, investigating mysteries, and helping hero's use data encryption, decryption and code breaking techniques. As part of this event, 260 families registered for 60 places. This event will be run annually with more information https://smarteduclub.com • Schools Capture the Flag Challenge – A beginner-friendly Capture-the-Flag event, where schools teams compete alongside a College level event. https://zerodays.ie/schools.html
		P – M13	Cyber Skills has led the promotion/development of cybersecurity skills for young professionals (age 18-24) by preparing an Irish team to participate in World Skills competition. This team is sponsored by Janssen Ireland and travelled to Korea in Oct 2022 (https://www.techcentral.ie/janssen-sciences-sponsor-worldskills-ireland-cybersecurity-competition/
		P – M13	Cyber Skills secured funding under SFI Science week to host a discussion about the safety of online shopping and social platforms with a mainly female audience. This conversation was held over Instagram with RTE presenter Anna Daly and Cyber Skills lecturer Gillian O'Carroll.
		P – M14	To respond to measure 14, in 2020 SFI engaged with academic community from MTU, UCD and cyber Ireland to understand the context of why Ireland needed a large scale investment in cybersecurity research, the scale of the proposed entity and an outline research programme. The responding team engaged

			with academic stakeholder from SFI research centres, IDA, EI, DEBI and the NCSC. The output of this engagement was subsequently submitted to SFI for further consideration and response.
10	Enterprise Development	P	In the section Progress to Date there is an error in the submission from Cyber Ireland referring to the report "State of the Cyber Security sector". This report was jointly published by Cyber Ireland and Cyber Skills. This should be updated and the error corrected. https://cyberskills.ie/explore/cyber-security-sector-report/
12	Citizens	FM	Form a cyber security citizens awareness group that focuses on developing awareness campaigns for the public and business, linking key stakeholders i.e. Cyber Skills, Garda Síochána, NCSC and other initiatives funded by government to raise awareness among citizens of the cyber security risk.
		P – M20	Cyber Skills formed a partnership with Safe Ireland to develop a billboard campaign highlighting the dangers of technology facilitated abuse. This partnership forms part of advancing cyber safe practices for young people using technology on a daily basis. https://www.safeireland.ie/learn-the-red-flags-of-technology-facilitated-abuse
		P - M20	Cyber Skills launched *CheckMyLink* (check.cyberskills.ie). This is a new national service that will be led by Cyber Skills in association with Scam Advisor and An Garda Síochána. The aim is to increase consumers' confidence that an online website that they are buying from is authentic, and to make sure that the website is not infected with malware. The service is easy to use and simply asks online users to provide only the URL of the website they are visiting. The service then generates an online report from trusted sources which is aimed at increasing consumers' confidence that the website or link, is authentic and safe to browse.