Rialtas na hÉireann
Government of Ireland

National Cyber Security Strategy 2019-2024 Mid-Term Review

May 2023

Prepared by the Department of the Environment
Climate and Communications
decc.gov.ie

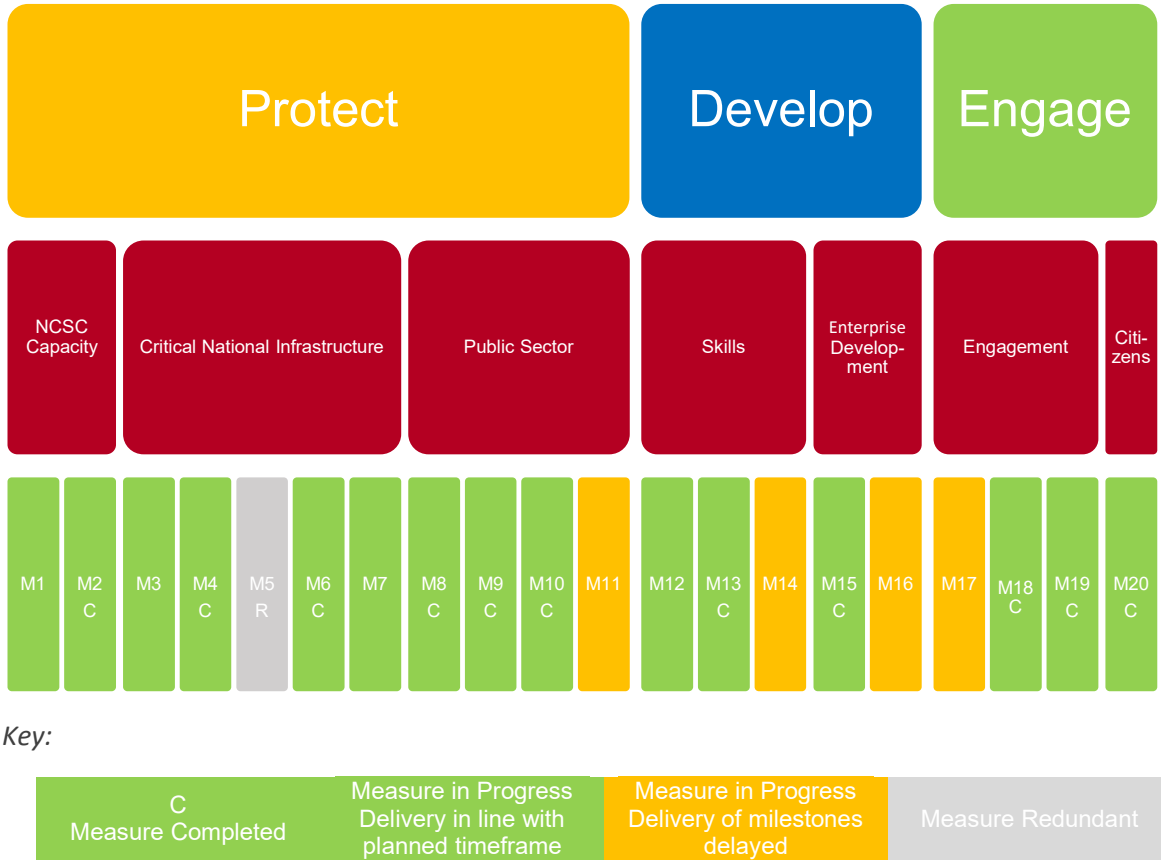
Contents

1. Introduction

The security and resilience of network and information systems is vital for Ireland's continued security and prosperity. Critical national infrastructure and essential services rely on complex systems and data flows which are vulnerable to attack by cyber criminals and other sophisticated threat actors. To maximise the impact of the ongoing green and digital transformations, it is vital that governments safeguard a secure, open, stable, and free cyber space from the ever-growing threat of malicious activity.

The National Cyber Security Strategy (NCSS), published in 2019, is a five-year whole of government strategy aimed at enhancing the security and resilience of Government systems and critical national infrastructure. The Strategy sets out a range of collaborative measures to enhance the cyber security and resilience of public bodies, providers of essential services, businesses, and households, to support the continued development of the cyber security industry and research community, and to ensure Ireland plays an active role in the international discussions on the security and stability of a free and open cyberspace. As the Figure 1 below illustrates, good progress is being made to implement the 20 Measures in the Strategy, and at the end of 2022, 12 of those Measures have been completed.

Figure 1: Strategy Overview



At its publication in 2019, the Government indicated its intention to review the Strategy at its mid-point to assess progress and consider new initiatives to ensure delivery across all the measures outlined therein. In 2021, a Capacity Review of the NCSC conducted by external consultants also recommended that the Strategy be reviewed in recognition of the changed global cyber threat landscape and evolution of the EU legislative framework. In December 2022, the Department of the Environment, Climate and Communications launched a public consultation on the Mid-Term Review of the National Cyber Security Strategy which closed on 7 February 2023. A series of stakeholder consultation webinars were hosted by the Department during January, as well as direct engagement with relevant Departments and State Agencies. Submissions to the public consultation will be published to the Department's website, together with summary notes of inputs at the stakeholder webinar sessions.

2. Vision

The 2019 Strategy was as follows.

> Our Vision is of an Irish society that can continue to safely enjoy the benefits of the digital revolution and play a full part in shaping the future of the internet. To that end, we will:
>
> **Protect** the State, its people and critical national infrastructure from threats in the cyber security realm in a dynamic and flexible manner, and in a way that fully respects the rights of individuals and proportionately balances risks and costs.
>
> **Develop** the capacity of the State, research institutions, businesses, the public sector and of the people to both better understand and manage the nature of the challenges we face in this space and to ensure that businesses and individuals can continue to benefit from economic and employment opportunities in information technology, and in particular in cyber security.
>
> **Engage** nationally and internationally in a strategic manner, supporting a free, open, peaceful and secure cyber space, and ensuring that cyber security is a key component of our diplomatic posture across the full range of engagement.

Recognising significant developments both internally and externally during the period 2019-2022, the Government proposed to revise the Pillars for the Strategy. The consultation paper highlighted the deteriorating threat landscape in which cyber security incidents are affecting a broader range of entities including small and medium-sized enterprises, education providers, and the community and voluntary sector. The consultation paper also referred to the importance of the European Union's Cyber Security for the Digital Decade strategy and associated legislative files, and in particular the expansion of the regulatory framework associated with the revision of the Network and Information Security Directive. The proposed review was met with general approval in the public consultation.

The revised Pillars in the Strategy are as follows:

Protect the State, its people, critical national infrastructure, and strategically important industry sectors, from threats in the cyber security realm in a dynamic and flexible manner, and in a way that fully respects the rights of individuals and proportionately balances risks and costs.

Develop the capacity of the State, education and research institutions, businesses including small and medium-sized enterprises, the public sector, the community and voluntary sector, and of the people to both better understand the manage the nature of the challenges we face in this space and to ensure that organisations and individuals can continue to benefit from economic and employment opportunities in information technology, and in particular in cyber security.

Engage nationally and internationally in a strategic manner, supporting a free, open, peaceful and secure cyber space, including playing an active role in the development and implementation of EU policy on cyber security, and ensuring that cyber security is a key component of our diplomatic posture across the full range of engagement.

3. New Measures

Government will, over the period 2023-2024, implement the following systematic measures to protect our nation, to develop our cyber security sector, and to deepen our international engagement on the future of the internet.

New Measures	
Measure 1	Continue to invest in the National Cyber Security Centre to expand its capacity to fulfil its mandate and ensure the NCSC has the required legal authority and technical capability to fully implement the revised Network and Information Security (NIS2) Directive from October 2024.
Measure 2	Continue to develop NCSC's ability to actively detect and defeat cyber threats targeting critical infrastructure and critical networks, including Government.
Measure 3	The NCSC will establish and lead a National Counter-Ransomware Task Force to coordinate efforts to respond to this severe cyber threat.
Measure 4	Develop an expanded programme of joint training and exercises between the NCSC, An Garda Síochána and the Defence Forces, to foster collaboration and enhance organisational capacity.
Measure 5	Develop further sectoral information sharing networks with relevant operators of critical national infrastructure and important industry sectors including Digital Infrastructure and Energy Sectors
Measure 6	Conduct an inter-agency risk assessment on supply chain risks including risk associated with relevant vendors in critical infrastructure, important industry sectors and the public sector[1], and make recommendations for Government on an appropriate policy response.
Measure 7	Establish a supervisory and enforcement regime for the revised EU Network and Information Security Directive (NIS2) and designate relevant bodies as National Competent Authorities and the Single Point of Contact.
Measure 8	Provide the NCSC with the necessary legal authority and technical capabilities to carry out security assessments of ICT systems for the handling of sensitive and confidential data.
Measure 9	Facilitate the ongoing development of a centralised repository of

[1] This measure will span CNI Protection and Public Sector Data and Networks. Propose that its scope should be those sectors within Annex 1 of the NIS Directive.

	educational and apprenticeship courses in cybersecurity at all levels and throughout the country, and use this data to develop materials for schools, guidance counsellors and others to raise awareness of careers in cyber security and learning pathways.
Measure 10	Undertake market analysis for cyber skills to better understand supply and demand, the effectiveness of current interventions and priorities for future policy and strategy.
Measure 11	Support the development of the Irish cyber security research community to develop its capacity with a view to delivering a significant initiative in Cyber Security Research (Measure 14 of the 2019 Strategy).
Measure 12	Within the framework of the Government's strategy for digital, develop a whole-of-Government strategy for the development of the cyber security industry in Ireland to ensure the sector achieves its potential for growth.
Measure 13	Implement a financial support programme for SMEs and other societal stakeholders, in accordance with EU provisions, to improve cybersecurity resilience and facilitate innovation
Measure 14	Develop a voluntary cyber security standard for Irish SMEs aligned with relevant international standards
Measure 15	Publish Ireland's national position on the application of international law in cyberspace, to contribute to international efforts to clarify the applicable legal framework and promote responsible State behaviour in cyberspace.
Measure 16	Develop and publish on a more frequent basis tailored advice and guidance documents on steps that can be taken by citizens, SMEs, schools and educational institutions, and community and voluntary organisations to prevent and mitigate cyber security risks.
Measure 17	Establish an NCSC Advisory Council to be drawn from the cyber security industry and research community, as well as representatives of key stakeholders, to provide independent perspectives and input on strategy and policies.
Measure 18	From 2023, publish an annual update on the implementation of this Strategy, to ensure accountability and transparency in the delivery of these Measures.

4.1 National Capacity Development

2019 Strategy Measures	
The National Cyber Security Centre will be further developed, particularly with regard to expand its ability to monitor and respond to cyber security incidents and developing threats in the State.	Ongoing
Threat intelligence and analysis prepared by the National Cyber Security Centre will be integrated into the work of the National Security Analysis Centre.	Completed

Update on Existing Measures

The Government has agreed a significant expansion of the NCSC, increasing headcount in the Centre to at least 70 by the end of 2024. Progress is well-advanced and the current NCSC headcount is 52. A permanent HQ facility for the NCSC is currently being developed as part of the redeveloped Departmental HQ at Beggar's Bush in Dublin 4 and is expected to be completed early in 2024. The proposed Joint Security Operations Centre will be developed as part of the new NCSC HQ facility. The NCSC is at present housed in temporary accommodation equipped with all necessary security and ICT provisions for the NCSC to fulfil its mandate. The NCSC is developing a graduate internship programme to be launched in 2023. Formal reporting and information sharing arrangements have been established with the National Security Analysis Centre.

New Measures

The public consultation emphasised that investment in developing the capacity of the NCSC should be linked to the evolving cyber threat landscape. The proposed Counter-Ransomware Task Force will identify and implement appropriate policy levers to prevent and mitigate incidents and undermine the ransomware business model. Stakeholders also emphasised that the capacity development process should also be responsive to emerging threats and consider emerging technologies such as artificial intelligence (AI). In addition, joint training and exercises between the NCSC, Defence Forces and An Garda Síochána will be continued during 2023 and 2024, including participation in international exercises.

New Measures	
Measure 1	Continue to invest in the National Cyber Security Centre to expand its capacity to fulfil its mandate and ensure the NCSC has the required legal authority and technical capability to fully implement the revised Network

	and Information Security (NIS2) Directive from October 2024.
Measure 2	Continue to develop NCSC's ability to actively detect and defeat cyber threats targeting critical infrastructure and critical networks, including Government.
Measure 3	The NCSC will establish and lead a National Counter-Ransomware Task Force to coordinate efforts to respond to this severe cyber threat.
Measure 4	Develop an expanded programme of joint training and exercises between the NCSC, An Garda Síochána and the Defence Forces, to foster collaboration and enhance organisational capacity.

4.2 Critical National Infrastructure Protection

2019 Strategy Measures	
The existing Critical Infrastructure Protection system flowing from the NIS Directive will continue to be deployed and developed, with particular focus on the ongoing compliance and audit programmes to mitigate risks to key services.	Ongoing
The NCSC, with the assistance of the Defence Forces and An Garda Síochána, will perform an updated detailed risk assessment of the current vulnerability of all Critical National Infrastructure and services to cyber attack.	Completed
The existing Critical National Infrastructure protection system will be expanded and deepened over the life of the Strategy to cover a broader range of Critical National Infrastructure, including aspects of the electoral system.	Redundant
The existing information sharing groups operated by the National Cyber Security Centre will be further developed, with the existing Threat Sharing Group being broadened to include a wider range of critical national infrastructure.	Completed
Government will introduce a further set of compliance standards to support the cyber security of telecommunications infrastructure in the State.	Substantially completed

Update on Existing Measures

The NCSC continues to deploy and develop the Critical National Infrastructure (CNI) protection system flowing from the EU Network and Information Security (NIS) Directive. The NCSC has published guidelines for Operators of Essential Services (OES) and works closely with them to identify and mitigate cyber risks affecting designated services, including through a programme of security audits. To prepare for the transposition of the revised NIS2 Directive, the NCSC has been engaging with relevant Departments and sectoral regulators to develop a proposal for the supervisory and enforcement structure, recognising the considerable expansion in the number of entities within scope. As outlined in the Consultation Paper, the task of expanding the CNI protection system (Measure 5 in the 2019 Strategy) will be implemented through the transposition of NIS2.

In respect of telecommunications infrastructure, the Government has endorsed the 'EU 5G Security Toolbox' as the framework by which Ireland will secure its next generation

electronic communications networks. The Communications Regulation Act 2023 provides a legal framework for the implementation of strategic and technical measures to mitigate security risks associated with 5G networks. A series of Electronic Security Control Measures have been drafted in consultation with industry to address technical risks. The legislation provides a basis for the Minister for Communications to assess the risk profile of providers of electronic communications network equipment and, if required, to designate certain vendors as being "relevant vendors" under Part 3 of the Act. The Communications Regulation Act 2023 also provides for certain parts of electronic communications networks to be designated as being critical and certain powers which would ensure that relevant vendors would not be used in critical electronic communications networks.

The NCSC has also been working with the Department of Housing, Local Government and Heritage and the Houses of the Oireachtas Commission to support them in enhancing the security of aspects of our electoral system and in 2021, the NCSC issued guidance on cyber security for political parties and candidates.

New Measures

Feedback from stakeholders for the information sharing networks has been very supportive and, with additional resources in the NCSC, there is a strong case to expand these to additional sectors. The growing threat of supply chain attacks has been highlighted in cyber risk assessments conducted in Ireland and internationally, and so it is important that appropriate measures are implemented to respond to this threat. The establishment of a robust national supervisory and enforcement regime is vital for the effective implementation of the NIS2 Directive, particularly recognising the scale and importance of the digital services sector in Ireland. Moreover, the national cyber risk assessment conducted in 2022 emphasised the positive role an enhanced cyber security regulatory framework can play to prevent and mitigate the threat of cyber security incidents to State, essential infrastructure, and our economy. To support our stakeholders, the Government will launch a public information campaign in advance of the national implementation of the NIS2 Directive, to raise awareness and inform relevant bodies and enterprises of their obligations under the Directive.

New Measures	
Measure 5	Develop further sectoral information sharing networks with relevant operators of critical national infrastructure and important industry sectors including Digital Infrastructure and Energy Sectors.
Measure 6	Conduct an inter-agency risk assessment on supply chain risks including

	risk associated with relevant vendors in critical infrastructure, important industry sectors and the public sector[2], and make recommendations for Government on an appropriate policy response.
Measure 7	The NCSC will lead the transition to a new supervisory and enforcement regime for the revised EU Network and Information Security Directive (NIS2) with sectoral regulators designated as National Competent Authorities in the transposition of the Directive.

[2] The scope of this risk assessment will cover those sectors within Annex 1 of the NIS Directive.

4.3 Public Sector Data and Networks

2019 Strategy Measures	
The NCSC will develop a baseline security standard to be applied by all Government Departments and key agencies.	Completed
The existing 'Sensor' Programme will be expanded to all Government Departments, and an assessment will be conducted by the same date as to the feasibility of expanding Sensor to cover all of Government networks.	Completed
A Government IT Security forum will be created, open to all Heads of IT Security across Government, to facilitate information sharing on best practice for cyber security and to allow the NCSC support the deployment of the baseline security standard.	Completed
The NCSC will be tasked by Government to issue Recommendations with regard to the use of specific software and hardware on Government IT and telecommunications infrastructure.	Ongoing

Update on Existing Measures

The NCSC's "Sensor" programme has been expanded to cover all Government Departments. The NCSC and the Office of the Government Chief Information Officer (OGCIO) published the Baseline Cyber Security Standard for Public Sector Bodies in November 2021. These standards set out a framework to be used by Departments and state agencies as a baseline to gauge their organisation's cyber security preparedness. They are based on the US National Institute of Standards and Technology and relevant European and international standards.

Building on the success of the steering group which developed the Baseline Standard, the NCSC has recently established the Government Cyber Security Coordination and Response Network (Gov CORE), which is a group of senior ICT security managers to provide guidance and support for the implementation of the Baseline Standard, and prepare for, and coordinate during, a major cyber security incident affecting government networks. In addition, the CORE Network pools resources, knowledge, experience, expertise, and training, to raise the overall level of security across Government Departments and networks. An online information-sharing platform has also been established as a resource to support the work of the Gov CORE Network.

The NCSC and the Office of the Government Chief Information Officer (OGCIO) are presently collaborating on a project to develop recommendations for the procurement of

software, hardware and cloud computing services on Government IT and telecommunications infrastructure, which will be published in the coming months.

New Measures

The transposition of the NIS2 Directive will have a significant impact on how public sector networks and systems are secured, as public bodies of central government will be Essential Entities and subject to supervision in common with operators of critical national infrastructure. The Directive makes provision for Member States to define the public bodies within scope more broadly, and the Government will consider and agree the national approach when publishing draft Heads of a Bill to transpose the Directive. Recognising the importance of securely handling sensitive and confidential data, the NCSC will take on a new role in certifying communication and information systems aligned with international best practice. In this regard, the Government will look to establish Information Assurance Authority and TEMPEST Authority functions within the NCSC remit.

New Measure	
Measure 8	Provide the NCSC with the necessary legal authority and technical capabilities to carry out security assessments of ICT systems for the handling of sensitive and confidential data.

4.4 Skills

2019 Strategy Measures	
Government will continue to ensure that second and third level training in computer science and cyber security is developed and deployed, including by supporting the work of Skillnets Ireland in developing training programmes for all educational levels and supporting SOLAS initiatives for ICT apprenticeship programmes in cyber security.	Ongoing
Science Foundation Ireland (SFI) will promote cyber security as a career option in schools and colleges by means of their Smart Futures Programme.	Completed
Science Foundation Ireland along with DBEI and DCCAE, will explore the feasibility through the SFI Research Centre Programme, the Research Centre Spoke programme or other enterprise partnership programmes to fund a significant initiative in Cyber Security Research.	Ongoing

Update on Existing Measures

There continues to be significant growth in the number of places available on cyber security courses at third level institutions and further education centres, a number of which are actively collaborating with industry partners. Science Foundation Ireland has incorporated cyber security as a career option in its Smart Futures Programme delivered in schools and colleges. This programme provides information on the range of career opportunities available in the field and has a particular focus on promoting STEM careers to girls and young women. A Cyber Security Education Working Group has been established and is overseeing a pilot Junior Cycle Short Course in Cyber Security.

In respect of cyber security research, a number of workshops were convened by Science Foundation Ireland (SFI) to explore opportunities for collaboration on a significant research initiative. While it has not been possible to identify a specific initiative for research funding thus far, SFI is supporting a number of research projects with a strong link to cyber security at institutions throughout the country.

New Measures

Cyber security skills was the most commonly highlighted issue in written responses to the public consultation and it was also considered in detail in the stakeholder webinars. While considerable progress has been since 2019, stakeholders highlighted challenges with hiring and retaining staff with critical skillsets. Educational providers also pointed to the importance

of cyber education at primary and secondary levels, to equip children and young people with the tools they need to stay safe online, and to raise awareness of cyber security career opportunities. The Government remains committed to funding a significant research project during the lifetime of the Strategy and the public consultation emphasised the importance of investing in the capacity of our research community. A number of practical measures have been identified which can have a positive impact during 2023 and 2024.

The Measures will build upon the existing collaborative relationships between the NCSC, Department of Education, Department of Further and Higher Education, Research, Innovation and Skills, Science Foundation Ireland, Technology Ireland ICT Skillnets, SOLAS, Cyber Ireland, and the educational and research institutions. They will inform the development of a new national cyber security industry strategy (Measure 11).

New Measures	
Measure 9	Facilitate the development of a centralised repository of educational and apprenticeship courses in cybersecurity at all levels and throughout the country, and use this data to develop materials for schools, guidance counsellors and others to raise awareness of careers in cyber security and learning pathways.
Measure 10	Undertake market analysis for cyber skills to better understand supply and demand, the effectiveness of current interventions and priorities for future policy and strategy.
Measure 11	Support the development of the Irish cyber security research community to develop its capacity with a view to delivering a significant initiative in Cyber Security Research (Measure 14 of the 2019 Strategy).

4.5 Enterprise Development

2019 Strategy Measures	
Government will continue to support and fully engage with the IDA funded Cyber Ireland Programme and explore new mechanisms to support Industry/Academia/Government cyber security collaboration.	Completed
Enterprise Ireland will develop a cyber security programme to facilitate collaborative links between enterprise and the research community that lead to the practical application of research in business.	Ongoing

Update on Existing Measures

The growth of the industry cluster Cyber Ireland has been a major outcome of the Strategy, with support from the NCSC, IDA Ireland, and Enterprise Ireland. The cluster's membership includes indigenous and multinational firms from both the pure-play cyber security and digital services sectors, as well as educational and research institutions. Particular highlights include the hosting of annual conferences in 2021 and 2022, and the publication last year of a report on the cyber security industry in Ireland and a position paper with recommendations for Government policy.

At a European level, progress is continuing to establish the European Cyber Security Competence Centre and Network pursuant to Regulation (EU) 2021/887. The Competence Centre will play a leading role in supporting the development of the European cyber security industry, including through the disbursement of EU funds for cyber security from the Horizon Europe and Digital Europe programmes. These funds will support enterprise development, research and development, as well as investment in national capacity building and cyber resilience. The Competence Network will bring together stakeholders from the industry and research communities to foster collaboration and information exchange. The Government has decided that the NCSC will act as Ireland's National Coordination Centre, with the support of Cyber Ireland. This Centre will play a vital role in establishing Ireland's Competence Network and facilitating engagement with the European Competence Network and access to the EU funding programmes for cyber security.

New Measures

A key message from the public consultation was the need to take a whole-of-Government approach to supporting cyber security enterprises. Stakeholders highlighted the breadth of activities underway and the roles that many government agencies can play to support the growth of the cyber security sector. The NCSC's Capacity Building team has established a

cross-Government task force to develop a new cyber security industry strategy which will be a vital component of the successor to the 2019 Strategy for the period from 2024 onward. The Government will continue to support Cyber Ireland to play a leading role in shaping the future development of this critical sector, and in particular in forging links between business and the research community.

Another significant focus of the responses to the public consultation was the need to support SMEs which have seen an exponential increase in the number of cyber security incidents since 2019. The NCSC will expand its services to support SMEs, by rolling out a grant funding programme to support cyber security investment and developing a voluntary cyber security standard tailored to the particular needs of SMEs. The NCSC will also assess options to develop a certification scheme based on this standard during 2024, which may be implemented as part of the post-2024 Strategy.

New Measures	
Measure 12	Within the framework of the Government's strategy for digital, develop a whole-of-Government strategy for the development of the cyber security industry in Ireland to ensure the sector achieves its potential for growth.
Measure 13	Develop a voluntary cyber security standard for Irish SMEs aligned with relevant international standards
Measure 14	Implement a financial support programme for SMEs and other societal stakeholders, in accordance with EU provisions, to improve cybersecurity resilience and facilitate innovation

4.6 Engagement

2019 Strategy Measures	
We will reinforce Ireland's diplomatic commitment to cyber security, including by stationing cyber attachés in key diplomatic missions and by engaging in sustainable capacity building in third countries.	Ongoing
We will create an interdepartmental group (IDG) on internet governance and international cyber policy to coordinate national positions across Departments	Completed
We will deepen our existing engagement in international organisations, including by joining the Cyber Security Centre of Excellence (CCD-COE) in Tallinn, Estonia.	Completed

Update on Existing Measures

With regard to appointment of cyber attachés in key diplomatic missions, the Government agreed that positions at the Permanent Representation to the EU in Brussels and the Irish Embassy in Washington would be prioritised. The Department of the Environment, Climate and Communications has approved the establishment of a new permanent, full-time attaché for cyber security in Brussels and the process of filling this post is underway at present. DECC and the Department of Foreign Affairs are working in partnership to progress the proposed attaché position in Washington.

An interdepartmental group on internet governance has been established, chaired by the Department of Foreign Affairs with representation from the Departments of Defence, Justice, DECC and the NCSC. The IDG meets regularly to coordinate policy positions across Government. Ireland has joined the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia and a member of the Defence Forces has been seconded to the Centre. In January Ireland formally joined the European Centre of Excellence for Countering Hybrid Threats in Helsinki and will have access to strengthen our capacity building to prevent and counter hybrid threats. The Government has also recently agreed to seek membership of the NATO MISP Smart Defence Project and the Microsoft Government Security Programme to complement existing information sharing platforms and threat feeds.

Work on the introduction of production and preservation orders, which would constitute significant progress towards enabling the ratification of the Budapest Convention, is ongoing. A General Scheme of a Bill will be published at the earliest date possible. Separately, the intention is that further legislative proposals to address the remaining elements of the

Convention will also be brought forward for the consideration of the Government later this year.

New Measures

The Government will continue to develop our cyber diplomatic footprint, through the placement of cyber security attachés in key diplomatic missions. Ireland will continue to have a strong voice in multilateral discussions on internet governance, supporting calls for a human rights-based approach to the development of the internet and digital technologies, including artificial intelligence. The publication of Ireland's national position paper on the application of international law in cyberspace will contribute to ongoing discussions at UN level and will promote responsible state behaviour in cyberspace and a more stable, secure, open, accessible and peaceful cyber environment with international law and the rules-based international order at its centre. Through our diplomatic network we will seek to assist more States to develop national positions on this important issue, including partners in the Global South. The Government will continue the ongoing process to prepare for the signature and ratification of the Budapest Convention.

New Measure	
Measure 15	Publish Ireland's national position on the application of international law in cyberspace, to contribute to international efforts to clarify the applicable legal framework and promote responsible State behaviour in cyberspace.

4.7 Citizens

2019 Strategy Measures	
Government will develop a national cyber security information campaign which will use information provided by the NCSC and the Garda National Cyber Crime Bureau and be delivered by entities which are directly engaged in information provision.	Completed

Update on Existing Measures

The NCSC and the Garda Cyber Crime and Financial Crimes Divisions regularly collaborate to disseminate information and guidance to help individuals prevent and mitigate cyber risks such as phishing, smishing, as well as measures to enhance the security of online banking and social media accounts. The NCSC and Garda Cyber Crime Bureau participate in the annual European Cyber Security Month campaign coordinated by the EU cyber security agency ENISA every October. The NCSC "Become Your Own Cyber Security Investigator" infographic developed for the 2020 campaign was recently awarded the Best Infographic Award by ENISA and translated into the 24 official languages of the EU for use in this year's campaign across the Union.

The Baseline Cyber Security Standard and other guidance for enterprises and organisations is available online to inform all citizens about measures that can be implemented at home, at school, and in community groups to prevent unauthorised access to systems and to secure personal and sensitive data.

New Measures

Responses to the public consultation and feedback at the stakeholder webinar sessions made a strong case for the Government to expand its cyber security information campaigns. While it was recognised that the annual European Cyber Security Month campaign was effective, respondents called for more information campaigns throughout the year. There was also an emphasis on developing tailored campaigns focused on specific communities, such as children and young people, the elderly, teachers and other educators, and community groups. Respondents also called for practical guidance to prevent and mitigate cyber security risks such as social engineering and data breaches, including advice on mobile phone security. These will be taken forward in a range of public information campaigns and materials hosted on the NCSC website.

New Measure	
Measure 16	Develop and publish on a more frequent basis tailored advice and guidance documents on steps that can be taken by citizens, SMEs, schools and educational institutions, and community and voluntary organisations to prevent and mitigate cyber security risks.

4.8 Governance Framework and Responsibilities

Progress to Date

The High-Level Interdepartmental Committee overseeing the implementation of the 2019 Strategy meets on a quarterly basis and is chaired by the Assistant Secretary for Communications in DECC. A progress report is prepared in advance of each meeting and relevant officials attend the meetings to provide detailed updates on progress. In line with the Government decision of July 2021, the IDC oversees the implementation of measures agreed in response to the NCSC Capacity Review including recruitment of additional staff and development of a dedicated HQ facility.

New Measures

There was strong support from stakeholders for the establishment of an Advisory Council for the NCSC, so this will be taken forward in the forthcoming legislation for the NCSC. The draft Heads of the Bill will set out the proposed role of the Advisory Council as well as relevant governance provisions such as the process for appointing members. Stakeholders welcomed the detailed account of delivery of measures to date in the public consultation document, and called for more frequent reporting for accountability and transparency. The proposed annual report will respond to these calls and the first will be published later this year.

The membership of the IDC overseeing the implementation of the Strategy will be refreshed to ensure participation by all relevant Departments. In response to a request from stakeholders, the IDC will also establish a number of thematic workstreams to ensure participation of key stakeholders in the delivery of relevant measures, e.g. State Agencies and other public bodies, academic institutions, and industry representatives.

New Measures	
Measure 17	Establish an NCSC Advisory Council to be drawn from the cyber security industry and research community, as well as representatives of key stakeholders, to provide independent perspectives and input on strategy and policies.
Measure 18	From 2023, publish an annual update on the implementation of this Strategy, to ensure accountability and transparency in the delivery of these Measures.

5. Development of Post-2024 Strategy

The five-year National Cyber Security Strategy was published in December 2019 and as this document notes, considerable progress has been made in the implementation of the 20 measures set out therein. This Mid-Term Review includes a further 16 measures to be implemented before the end of 2024. Following on from that, it is proposed that a successor strategy – the third National Cyber Security Strategy – will be published to set out the Government's vision for cyber security in the State and the measures to be implemented to deliver this vision.

The NIS2 Directive referenced earlier includes provisions for national cyber security strategies, including a number of areas Member States required to consider when drafting their national strategy. The relevant article will be transposed into Irish law as part of the transposition of the Directive, and so it will inform the process of developing the successor strategy for the period from 2024 onwards.

The responses to the public consultation included a range of ambitious proposals for Government to consider, many of which will require more than two years to implement. These contributions are welcome and they will inform the development of the successor strategy. The process of strategy development will commence during 2024 and will include a further public consultation as well as stakeholder engagement. To prepare for this process, it is proposed to conduct a foresight analysis of the political, economic, technological, and legal trends in cyber security at national and international level. This will be led by DECC in consultation with IDC members and other relevant stakeholders.

6. Mid-Term Review Table of Measures and Milestones

Protect					
No.	**Priority Area**	**Measure**	**Lead Dept/Agency**	**Support Dept/Agency**	**Milestones for Delivery**
1	National Capacity Development	Further invest in the National Cyber Security Centre to expand its capacity to fulfil its mandate and ensure the NCSC has the required legal authority and technical capability to fully implement the revised Network and Information Security (NIS2) Directive from October 2024.	DECC	DPER, PAS, AGO	Staffing Complement in NCSC will be at least 80 WTE by the end of 2024. Legislation to be enacted to transpose the NIS2 Directive and grant relevant mandate and legal authority to the NCSC before 16 October 2024. Delivery of priority measures in the NCSC Technology Strategy required for implementation of the NIS2 Directive by the end of October 2024.
2	National Capacity Development	Continue to develop NCSC's ability to actively detect and defeat cyber threats targeting critical infrastructure and critical networks, including Government.	DECC		Heads of a Bill will be drafted for Government approval by year-end 2023. Recruitment of personnel with relevant expertise and skills before year-end 2024. Implementation of priority measures in the NCSC Technology Strategy before year-end 2024.
3	National Capacity Development	The NCSC will establish and lead a National Counter-Ransomware Task Force to coordinate efforts to respond to this severe cyber threat.	DECC	DOJ, DFA, DOF, AGS, CBI	Task Force to be convened and work programme Agreed before year-end 2023.

					4 quarterly meetings to be held during 2024 to progress delivery of work programme.
4	National Capacity Development	Develop an expanded programme of joint training and exercises between the NCSC, An Garda Síochána and the Defence Forces, to foster collaboration and enhance organisational capacity.	DECC	DF, AGS, DOD, DOJ	Expanded programme to be scoped and proposals developed before the end October 2023. The first annual programmes of joint training and exercises will be agreed before year-end 2023 and implemented during 2024.
5	CNI Protection	Develop further sectoral information sharing networks with relevant operators of critical national infrastructure and important industry sectors including Digital Infrastructure and Energy Sectors	DECC		2 additional sectoral information sharing networks will be established before the end of 2023. Following establishment, quarterly meetings of the networks will be convened.
6	CNI Protection	Conduct an inter-agency risk assessment on supply chain risks including risk associated with relevant vendors in critical infrastructure, important industry sectors and the public sector[3], and make recommendations for Government on an appropriate policy response.	DECC	NSAC, DOD, DOJ, DFA, OGCIO, CBI, AGS, DF	Inter-agency task force will be established by Q1 of 2024. Risk assessment completed and recommendations presented to Government before the end of Q4 2024.
7	CNI Protection	Establish a supervisory and enforcement regime for the revised EU Network and Information	DECC	Relevant Departments	Proposals for the supervisory and

[3] This measure will span CNI Protection and Public Sector Data and Networks. Propose that its scope should be those sectors within Annex 1 of the NIS Directive.

		Security Directive (NIS2) and designate relevant bodies as National Competent Authorities and the Single Point of Contact		and Agencies	enforcement regime will be presented to Government before the end of Q3 2023. A working group of relevant Departments and agencies will be convened in Q3 2023 to prepare for transposition and implementation of the Directive. Draft Heads of a Bill to transpose the NIS2 Directive designating will be prepared before year-end 2023. Process of transposition will be completed before the deadline of 16 October 2024.
8	Public Sector Data and Networks	Provide the NCSC with the necessary legal authority and technical capabilities to carry out security assessments of ICT systems for the handling of sensitive and confidential data.	DECC	DOJ, DOD, DFA	Heads of a Bill will be drafted for Government approval by year-end 2023. Legislation to be in place by the end of 2024. Recruit relevant staff and other necessary administrative measures completed before year-end 2024.
Develop					
9	Skills	Facilitate the ongoing development of a centralised repository of educational and apprenticeship courses in cybersecurity at all levels and throughout the country, and use this data to develop materials for schools, guidance	DECC	DFHERIS, DOE, Solas, ICT Skillnet, HEA, Cyber Ireland,	Scoping exercise on the proposed repository to be completed before year-end 2023. Options for development of

		counsellors and others to raise awareness of careers in cyber security and learning pathways.		PDST	the repository to be presented to IDC for consideration before end Q1 2024. Repository established by Q3 2024. Materials for schools and guidance counsellors to be published before year-end 2024.
10	Skills	Undertake market analysis for cyber skills to better understand supply and demand, the effectiveness of current interventions and priorities for future policy and strategy.	DECC	DFHERIS, Solas, ICT Skillnet, HEA, Cyber Ireland	Terms of Reference and scope for market analysis to be agreed before end Q3 2023. Procurement of consultancy services to be completed in Q4 of 2023. Market analysis completed before end Q2 2024 and recommendations for future policy and actions presented to IDC for consideration in the context of post-2024 Strategy.
11	Skills	Support the development of the Irish cyber security research community to develop its capacity with a view to delivering a significant initiative in Cyber Security Research (Measure 14 of the 2019 Strategy).	DECC	DFHERIS, SFI, Cyber Ireland	Scoping of support measures to be completed before the end of Q3 2023 and proposals presented to IDC for consideration. Support measures to be implemented before year-end 2024.
12	Enterprise Development	Within the framework of the Government's strategy for digital, develop a whole-of-Government strategy for the development of the	DECC	DETE, DFHERIS, DoE, IDA,	Cross-government steering group to be established before the end of Q2 2023.

		cyber security industry in Ireland to ensure the sector achieves its potential for growth.		Enterprise Ireland, SFI, HEA, Solas, Technology Ireland, Cyber Ireland	Procurement of consultancy services to be completed in Q3 of 2023. Strategy will be drafted and presented to the IDC before the end of Q1 2024.
13	Enterprise Development	Implement a financial support programme for SMEs and other societal stakeholders, in accordance with EU provisions, to improve cybersecurity resilience and facilitate innovation	DECC	DETE, Enterprise Ireland	Stakeholder engagement to be conducted during Q3 2023. Subject to approval of EU funding (for NCC-IE project), call for funding applications to be opened in Q1 of 2024. Applications to be reviewed and approved during Q2 and Q3 of 2024. Grants to be awarded before year-end 2024.
14	Enterprise Development	Develop a voluntary cyber security standard for Irish SMEs aligned with relevant international standards.	DECC	NSAI, Enterprise Ireland, Cyber Ireland	Scoping exercise for SME cyber security standard to be conducted and proposals presented to IDC in Q4 of 2023. Voluntary standard to be published in 2024.
Engage					
15	Engagement	Publish Ireland's national position on the application of international law in cyberspace, to contribute to international efforts to clarify the applicable legal framework and promote responsible State behaviour in cyberspace.	DFA	NCSC/DECC, DOD, DOJ, AGO	National position published before year-end 2023.
16	Citizens	Develop and publish on a more frequent basis tailored advice and guidance documents on steps that can be taken by citizens, SMEs, schools and	DECC	AGS, DETE, DOE, DFHERIS,	Scoping on public awareness activities to be conducted in Q3 of 2023

		educational institutions, and community and voluntary organisations to prevent and mitigate cyber security risks.		DRCD, Enterprise Ireland, HEA, Solas	and proposals presented to the IDC. An annual public awareness programme will be agreed by the IDC in Q4 of 2023 and delivered during 2024. Stakeholders will be surveyed before the end of 2024 to measure impact of the public awareness programme and inform development of future programmes.
Governance and Oversight					
17	Governance	Establish an NCSC Advisory Council to be drawn from the cyber security industry and research community, as well as representatives of key stakeholders, to provide independent perspectives and input on strategy and policies.	DECC		Terms of reference for the Advisory Council to be agreed before year-end 2023. Heads of a Bill to establish an Advisory Council drafted for Government approval by year-end 2024. Proposal for appointing members to the Advisory Council to be presented to the IDC before year-end 2024.
18	Oversight	From 2023, publish an annual update on the implementation of this Strategy, to ensure accountability and transparency in the delivery of these Measures.	DECC	IDC Participants	First annual update drafted for consideration by the IDC in Q4 of 2023. Second annual update drafted for consideration by the IDC in Q4 of 2024.