

Cisco response to National Cyber Security Strategy 2019-2024 Mid-Term Review Consultation

7 February 2023



Disclaimer

Thank you for the opportunity to submit this response to this Inquiry. Cisco is not responsible for any inadvertent errors in our response.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)



Table of Contents

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY 1

- Key recommendations for the Strategy 1**

INTRODUCTION..... 3

- Vision 3**
- Objectives 4**
- National Capacity Development 5**
- Critical National Infrastructure Protection 6**
- Public Sector Data and Networks..... 8**
- Skills 8**
- Enterprise Development..... 9**
- Engagement..... 10**
- Citizens 10**
- Governance Framework and Responsibilities 10**
- Conclusion..... 11**
- Where Cisco can help..... 12**





Executive summary

Cisco welcomes Ireland's significant progress in developing its cyber security capability since the inception of the current National Cyber Security Strategy in 2019, which reflects the ever-increasing prevalence of cyber issues across both the public and private sector in the intervening period. As demonstrated by the attacks on the HSE in 2021, it is hugely important for the NCSC and Ireland's public and private sector organisations to strengthen their capacity to prevent such attacks in the future. Given the rapid speed at which the cyber landscape is changing, it is crucial that the State engages in regular two-way dialogue with stakeholders to consistently strengthen and optimise the NCSC's and Ireland's overall approach to cybersecurity.

At this midway point in the current Strategy, Cisco believes that there are a number of areas where Ireland could further strengthen and update measures to support the achievement of objectives under the Strategy. These are summarised below and outlined in further detail in the submission.

Key recommendations for the Strategy

Cisco broadly welcomes the aims of the Strategy and the roll-out of associated implementation measures to date, as well as those still to come in the coming months and years. However, as part of the mid-term review of the strategy, there are a number of areas where we believe the State, and by extension the NCSC, can optimise the efficacy of Ireland's cybersecurity actions and objectives. Among the key recommendations are as follows:

1. Ensuring greater **investment** in the State's cyber capacity (beyond the NCSC) by ensuring adequate allocation of resources for improving the cyber infrastructure across the entire public sector;
2. Continuing to attract investment in cyber in Ireland by ensuring **regulatory consistency, alignment and harmonisation** with the rest of the EU;
3. Promoting a **secure by default approach** to all software and hardware products in Ireland;
4. Adopting a holistic approach to cyber protection by ensuring **entire supply chains are in scope** of all cybersecurity initiatives and requirements;
5. **National Capacity Development:** further consideration is needed regarding the Coordinated Vulnerability Disclosures, e.g. for organisations working with third parties
6. **Critical National Infrastructure Protection:** consider the possibility of self assessment with regards to vulnerability assessments, given the significant work required and the limited resources of the NCSC. Further clarity is needed on the obligations of Operators of Essential Services under NIS2, as well as on how the NCSC envisages the plan for threat intelligence sharing.

-
7. Invest further in **cybersecurity skills** for citizens, not only for second and third level students, but also in adult further education and vocational training.
 8. Engagement: continue **international engagement** on cybersecurity matters, and develop greater cooperation with the Ireland/EU cooperation with the UK on cyber.
 9. Governance Framework & Responsibilities: take advantage of the extensive cyber knowledge in Ireland, by **involving industry in cyber structures**, e.g. the Strategic Advisory Group of Cybersecurity Research Stakeholders.

Introduction

Cisco UK and Ireland (henceforth Cisco) welcomes the opportunity to submit written evidence to the public consultation on the mid-term review of the National Cyber Security Strategy 2019-2024. With nearly 30 years operating in Ireland, and sites in both Dublin and Galway, Cisco's Irish team possesses a wide variety of skills across many of our product offerings, including cloud software development, user experience, product management, marketing, program management, sales, and of course, cyber security. Cisco possesses a wealth of cyber security expertise drawn from an international network of experts, including Cisco Talos Intelligence Group which is one of the largest commercial threat intelligence teams in the world, comprised of world-class researchers, analysts and engineers.

As outlined in the Government's national digital strategy 'Harnessing Digital - The Digital Ireland Framework' and in recognition of the growing importance of cyber security, the State has rightly prioritised the development of Ireland's cyber security capacity, expertise, and infrastructure. Given the ever-changing nature of the cyber security landscape, it is important that actions and measures evolve in real time with developments and therefore this mid-term review offers a crucial opportunity to reflect on the efficacy of the strategy and its direction of travel in the coming months and years.

For national governments, cybersecurity has never been as important as it is today. The protection of our IT systems, data services and communication networks, is vitally important to governments and for the running of our economy and society. Disruption to our digital systems is not only expensive, but crucially also undermines trust and confidence in them. It is the government's role to develop policy and strategies which help us to safely use and enjoy digital communication and Cisco is happy to provide expertise to assist in this important work.

As demonstrated by our work with Government on skills training initiatives, Cisco is keen to collaborate with policymakers and share as much relevant knowledge and expertise as possible. Cisco has been collaborating closely with the State on several areas related to cyber security skills and we hope to continue and deepen this cooperation over the coming years and further expand it to other key areas in the cyber ecosystem.

Below you can find more detailed responses to the questions posed within the consultation paper, as well as a number of Cisco proposals put forward to address some of the cybersecurity challenges touched on throughout the consultation paper:

Vision

An evolving landscape

Given the ever-changing landscape of the cyber threat landscape and the evolving cyber ecosystem, it is crucial that Government policy and overall strategy on cyber security are reviewed on a regular basis, to test the overall objectives and strategy and ensure that the right measures are being pursued to proactively deliver on it. It is

important that a robust process is in place to regularly monitor the continued efficacy of the strategy including approaches that should be taken to adjust it accordingly. This mid-term review is a welcome exercise in this regard.

Cisco considers that the vision set out in the Strategy is still broadly relevant, however it could usefully be updated to encapsulate the role of public and private organisations in realising the vision.

At the same time, the overall strategy could be updated to include **increasingly relevant sectors in the Strategy, for example artificial intelligence (AI)** and quantum. Over the past decade, and in particular since the inception of the Strategy, both of these sectors have witnessed significant areas of advancement, which have impacted cyber more broadly. In light of these developments, Cisco believes that it may be of value to consider making explicit reference to these two areas, in order to ensure that the necessary focus is applied – regarding both the exploitation of the major benefits of these technologies in Ireland, but also to ensure adequate protection in the case of malicious use against Ireland.

Objectives

National Security Analysis Centre: Cisco welcomes the establishment of the National Security Analysis Centre (NSAC) as a way to ensure greater coordination between cybersecurity stakeholders in Ireland. To assist and supplement the work of the NSAC and improve its efficacy, we recommend the **creation of a high-level cybersecurity group to assist the NSAC**, which could comprise not just representatives from the Defence Forces, but also MNC specialists etc. This high-level group could review and revise standards on a frequent basis. With the proposed Strategic Advisory Group of Cybersecurity Research Stakeholders, the Government has demonstrated its willingness to involve external experts in the work of the NCSC, and the above-mentioned high-level group could act in a similar vein. Additionally, the Government should consider consulting industry stakeholders in the formation of such a group, given that they have extensive experience collaborating with researchers and academics on issues related to cybersecurity.

Secure by default: Cisco believes that an important objective for Ireland's approach to cyber security should be ensuring that **infrastructure suppliers adopt a 'secure by default' position for their products and services**. Too many cyber security vulnerabilities come about as a result of the systemic failure of technology suppliers to 'build-in' security to their products and services from the outset. Around the world, many national governments are engaging with industry on issues like Secure by Design to drive improvements in the security of technology supplied to both consumers and businesses. Notably the UK government has embedded this in its strategy and we believe that it is worth exploring in Ireland, potentially also in tandem with similar work being undertaken at EU level as part of the **Cyber Resilience Act**.

Crucially, a lack of consideration for cyber security issues has led to the wide-spread concerns currently seen around the **'Internet of Things'** marketplace, wherein a large and diverse set of new technology vendors move rapidly to gain first mover advantage, often at the expense of implementing robust security controls in their products. By 2025, it is estimated that there will be more than 21 billion IoT devices globally. Given this huge and rapid expansion of connected devices and by extension, the exponential increase in the quantity of data, by adopting and promoting a 'secure-by-default' approach, the Government can take a significant step towards ensuring that all new products do not threaten the safety and integrity of the overall cyber system.

Attracting investment: Cisco believes that one of the central objectives of Ireland’s cyber strategy needs to be attracting investment from the cyber industry by adopting a more outward looking position towards the whole industry, and crucially demonstrating to potential investors that Ireland is a safe place to invest. As outlined in the National Digital Strategy and repeated again in the recent progress report, the **government is committed to supporting those affected by recent job losses in the sector and maintain competitiveness by ensuring that Ireland is the best place in Europe to invest and grow for the future**, with cybersecurity a clear example of where such investment can and should occur. While the objective of attracting investment is partly covered in the current objectives of the Strategy, it is bundled in with the objective related to raising awareness inside business, however this needs to be more expansive and outward facing to attract further investment. Additionally, the focus appears to be primarily on investment in new technology, however again our belief is that the aspiration should be on both new technologies but also increasing investment in current technologies and systems.

Security across entire supply chains: While the issue of supply chain security is touched on in the review of the Strategy, we believe that there should be much more of an emphasis on the topic. The last few years has seen a major shift in focus to this area and therefore we believe that all Governments need to start building policies and guidance to help both themselves and businesses in navigating this complex but crucial field. **Supply chain security should be a central tenet of any comprehensive cybersecurity strategy**, allowing stakeholders to have the capacity to continually assesses, monitors, and improves the security throughout the entire lifecycle of any technology. There are multiple paths towards achieving this – for example by developing more effective procurement advice for Government and CNI, or alternatively by working with key strategic suppliers in the region.

Adopting the right approach to software: Similarly when it comes to assessing and addressing vulnerabilities, it is important that the Strategy ensures that there is significant consideration of **open-source software; an area where the extensive vulnerabilities have been well documented over the past few months** (Log4j being the most recent example of this). For that reason, governments around the world are exploring policy interventions in this area and therefore it is important that similar considerations are part of the Irish cybersecurity strategy. [REDACTED]

[REDACTED] Cisco has actively contributed to the international standards community that are critical in supporting the outcomes in the Order and are keen to share insights and experiences with the Government to help inform future policy in this important area.

National Capacity Development

Coordinated Vulnerability Disclosure: While the establishment of a Coordinated Vulnerability Disclosure (CVD) policy in the coming year(s) is a welcome development, particularly as a driver of standard behaviour in this area, there are several concerns that such a proposal raises - specifically the envisaged role of the NCSC to act as a coordinator and trusted intermediary between researchers and industry. While this is a requirement under the revised NIS Directive, there are several caveats that must be considered in its implementation and enforcement, for example the consideration that organisations may be working with third parties on such issues which could impact the disclosure process. Furthermore, it will also be important to consider the notification sequence of such

a process as once mitigation is in place, all relevant parties will need to be notified, meaning that there will be no prioritisation of certain Member States or bodies over others. Finally, while the Strategy envisages the NCSC acting as a coordinator and trusted intermediary between researchers and industry, given the urgency of such information, it is imperative that industrial stakeholders are prioritised in disclosure of the information.

Investment across the public sector: Cisco welcomes the major increase investment in the NCSC and the expansion in resourcing and headcount within the organisation. At the same time, we believe that there is a need for significantly more horizontal investment in cybersecurity infrastructure and education across the public sector – e.g., in health, public administration, finance, etc. – to ensure a holistic approach to cyber protection across the government and all State bodies.

Critical National Infrastructure Protection

Vulnerability assessments: Cisco welcomes the NCSC’s intention in 2023 to begin conducting vulnerability assessments of critical infrastructure in government. This will provide the opportunity to highlight where the most pressing vulnerabilities lie and thus undertake the appropriate corrective measures. Given that this is a process that has been carried out by other national authorities, it would be worthwhile for the NCSC to utilise the experience of their international colleagues.

However, given the significant undertaking that carrying out such assessments would entail – both in terms of resources and expertise - it will be important for the NCSC to determine whether they have the resources for conducting such assessments. While the increased resourcing and headcount within the NCSC is hugely welcome, before embarking on such assessment processes, it will be important for the organisation to consider whether its current and planned resourcing is sufficient to match the scale required for such vulnerability assessments. Prior to beginning the assessments, the NCSC will need to provide clarity about what will happen with the results of such tests – i.e. where and how long will they be stored, who will have access, etc., as well as what the actions proceeding from the culmination of such tests will be.

The NCSC should consider an approach whereby it **works with trusted partners in the cyber ecosystem to conduct these assessments**, and thus takes full advantage of the extensive expertise available to carry this process out. Such a step could align with other aims of the Cyber Security Strategy which highlights the importance of improving engagement with industry and developing closer cooperation with all relevant stakeholders. Furthermore, by compelling the cyber security sector to carry out a self-assessment and provide the results to the NCSC, this will not only allow the NCSC to allocate resources elsewhere but also ensure that companies are best placed to implement any measures stemming from the assessments.

UK Active Cyber Defence program: The [UK Active Cyber Defence program](#) is an excellent example of how a suite of simple tools can be used to make a very real impact on improving cyber resilience of the Governments’ Internet facing services. The program has built a new set of distinct capabilities which could easily be adopted by the Irish NCSC, such as:

- A **discovery capability** which aims to answer the simple questions, ‘What is the Government IT footprint on the Internet’?
- **Assessment tools** to look at both web and e-mail services which inspect them for weak or poor configuration practices and provide simple, actionable advice for remediation. For example, email infrastructure should focus on simple to implement security controls such as the Sender Policy Framework

(SPF) and Domain Message Authentication Reporting & Conformance (DMARC), the implementation of which can have a significant impact on the ability for cyber criminals to spoof Irish Government e-mail.

- A **protected DNS service** which blocks access to known malware and phishing domains for Government users. This can be delivered transparently at scale and provides protection against the known bad.

In order to ensure optimal efficacy, the NCSC should **prioritise its resources on supporting Government organisations where there is a higher threat and/or where higher classification information is being held**, e.g., Department of Defence or the Garda. To address the higher volume, lower threat departments, the NCSC should encourage **sharing of common, best practice blueprints**, meaning that when a department implements a solution to address a particular use-case, they should be encouraged to share this, as others will likely be facing similar problems in their own environments. This will encourage greater sharing and has the effect of scaling the limited cyber security expertise across the wider sector.

Critical infrastructure: many networks today are considered critical infrastructure, and essential to maintain economies and vital industries – everything from healthcare, energy, transport, government, financial services, and more. With the entry into force of the **NIS 2 Directive** this month (Jan 2023), Member States will need to ensure a safer and stronger Europe by significantly expanding the sectors and type of critical entities falling under its scope - including providers of public electronic communications networks and services, data centre services, wastewater and waste management, manufacturing of critical products, postal services, as well as the healthcare sector more broadly. In the coming months, it will be critical that the State ensures that providers have the appropriate **conformity with the NIS Directive**. Cisco believes that the best way to mitigate against an attack against critical infrastructure is to audit on a regular basis a critical infrastructure provider's cyber posture and conformance with the NIS 2 Directive.

Facilitating information and intelligence sharing within a network is crucial to achieving optimal levels of cyber security. In this regard, the UK again offers an excellent example of how such a process can be implemented in practice. The **UK model of sector-specific Information Exchanges and the Cyber Information Sharing Portal (CiSP)** work very effectively at enabling both general and sector specific threat information to be shared with confidence using the well-established Traffic Light Protocol.

Operators of Essential Services (OES): Overall Cisco welcomes that under NIS2, businesses identified by the Member States as operators of essential services in the above sectors will have to take appropriate security measures and notify relevant national authorities of serious incidents. With this, key digital service providers, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements as a means of ensuring that appropriate incident response plans are in place to reduce and manage any disruption to services

However, within NIS2 there remains a lack of clarity on several key issues, including in relation to the competent authorities for the implementation of certain security measures related to the OES. Additionally, within the text of the Directive it remains unclear what the requirements for organisations are on key issues, such as transparency obligations. Given this ambiguity and lack of clarity on a number of important issues, Cisco strongly recommends that ENISA should work closely with Member States on implementing and further developing these standards, and encourages Ireland to be a proponent of Member State involvement in the process to ensure a harmonised and realistic implementation process.

Threat intelligence sharing: Cisco welcomes the NCSC's objective of building a network of sectoral Information Sharing Networks, which will further substantiate the security and resilience of critical infrastructure through the

use of secure Cyber Threat Intelligence sharing platform. At the same time, it is important for the NCSC to recognise the need for reciprocity and security of such a network. It is imperative that the NCSC ensure that the information shared is subject to the highest security guarantees. Similarly, all organisations and businesses engaging with the platform should benefit from the cooperative nature of the information exchange by ensuring that there is an adequate trade-off in the risks that involvement in such a platform entails. Lastly, to ensure that the information exchanged on this platform can be used effectively and facilitate the evolution of the cyber security ecosystem, the use of the information by organisations should not be accompanied by extensively excessive or burdensome prerequisites.

Public Sector Data and Networks

Cisco fully supports the proposal for the NCSC to come forward with mandatory requirements for all entities who are providing cyber security services to the Irish public sector. The development of such standards would **align with the 'secure by default' concepts outlined in the proposed strategy objectives above** and help define a minimum set of security and assurance requirements covering aspects of product security that would have a meaningful impact on overall CNI resilience. This would include factors such as supplier secure development practices and robust engineering approaches.

Additionally, given that citizens are increasingly interacting with their public services through digital technology, the development and roll-out of such standards would help ensure that the **necessary level of trust is built and maintained**, in order to maximise engagement with future digital public services.

Skills

As highlighted in the mid-term consultation paper, **Cisco has been working closely with the Government on cyber skills training initiatives**, and hope to continue and deepen this cooperation over the coming years and further expand it to other key areas in the cyber ecosystem. A 2022 [study from the Centre for Economics and Business Research \(CEBR\)](#), commissioned by Cisco, found that a more inclusive digital economy that connects everyone in Ireland, equips them with digital skills, and digitises key industries and public services, has the **potential to add €28 billion to the Irish economy by 2030**. At the same time, the study identified a number of key barriers and risks to the digital transformation, including a “fear of cyber-crime” and highlighted the need for the government to support new and improved services and infrastructure in areas such as cybersecurity.

While the Strategy includes welcome initiatives focussed on building a skills pipeline from schools and universities, there is little emphasis on the need to incentivise and help those already in the workforce to move into a career in cyber security.

Our research indicates that to achieve digital inclusion in Ireland by 2030, where everyone can participate in a more digital society, **70,000 people a year must gain essential digital skills**, and additionally to build a more digital workforce, 131,000 need to develop a higher level of digital skills each year. This should include not only students and new graduate, but also those already in the workforce looking to move into cyber. Therefore, the Strategy's actions on Skills should also ensure funding and incentives for **further education and in-career training certifications**. With advances in skills, connectivity and digital adoption, it is estimated that **Irish industry would**

benefit from a boost to productivity in the region of €24 billion. Given this large increase in digital inclusion, ensuring adequate training and skills – both for students and adults – will be crucial for both the Irish State in the years to come.

With **2023 being the [EU Year of Skills](#)**, this presents a good opportunity to highlight the need for improving digital skills and training, including on cyber, across the EU. The Government should explore the various EU initiatives connected with the Year of Skills, in particular how this can align with the goals of the EU Digital Decade for 2030. The **Digital Decade Strategy** includes Skills among its key pillars and highlights the potential of multi-country projects, such as deploying a network of Security Operations Centres, powered by AI, to anticipate, detect and respond to cyberattacks at national and EU level. This demonstrates the multi-national approach that can be adopted with regards to cyber skills, and which should be a key issue in the Government’s cyber strategy in the coming years.

Additionally, Cisco welcomes the **cyber security graduate training programme**, initiated by the NCSC, which will be launched this year and pave the way for computer science graduates to be recruited each year, however there also needs to be a focus on in-career / vocational training for those already in the workforce looking to transition to a career in cybersecurity. Alongside such a graduate programme, the NCSC should consider supplementary means to further build capacity through the use of short-term secondments. Here the **UK NCSC offers a good example, where thanks to its [i100 \(Industry 100\) scheme](#)**, it has successfully fostered collaboration between public and private sector through placements of industry professionals within the organisation. Since its inception in 2017, the scheme has seconded 180 industry partners into teams across all areas of the NCSC, with 39 new participants taking up the opportunities in 2022 alone. Notably, participants included lawyers, analysts and chief technology officers for multinational cyber security companies, who joined NCSC teams on a part-time basis and as result, had a valuable opportunity to work on a range of strategic and tactical activities in the cyber space.

According to a [2021 report from Cyber Ireland and Cyber Skills](#), which identified 489 cyber security companies operating across the country, **Ireland has an opportunity to become a global leader in cyber security and to grow the workforce to over 17,000 by 2030.** In today’s ever-evolving job market, upskilling and reskilling have become essential to stay competitive, particularly in the technology industry, where advancements are happening rapidly. Currently there two major challenges in the cybersecurity field: the talent shortage and the skills gap. Cisco considers the talent shortage to be the lack of qualified cybersecurity talent – a shortage of people with a solid background in cybersecurity. This differs from the skills gap, which creates the need for continuing education and training to enable cyber security-savvy talent to keep up with ever-evolving cybersecurity threats. Given that both upskilling and reskilling will be crucial to the future of the cybersecurity sector in Ireland, measures and incentives promoting both should be considered as part of the Strategy moving forward – for example through Further Education Training, SkillNet and national apprenticeship programmes.

Enterprise Development

With the new requirements under NIS2 and the expansion of obligations for OES, in the coming months and years, there will be a clear need for increased investment (both indigenous and foreign) to ensure that Ireland has the capacities to deal with these new requirements. At the same time, this also provides the opportunity for developing the cyber industry in Ireland, thereby increasing the quantity of jobs and overall output of the cyber sector in Ireland as a whole.

Engagement

Cisco welcomes Ireland's the ongoing engagement in cyber security at both EU and UN level, as well as the setting up of the interdepartmental group on international cyber policy. Cybersecurity is inherently international in its scope and developments in recent years have demonstrated the need for states to place cyber at the core of their foreign and domestic policy agendas. Alongside the work being done at EU and UN level, Cisco welcomes the expansion of information sharing groups with UK CNI protection agencies.

Ireland, the UK and the EU are broadly aligned in their approach to the cyber space, however the impact of Brexit on the UK's membership of ENISA has undoubtedly affected EU-UK cooperation levels. For that reason, **greater cooperation and collaboration between Ireland, the EU and the UK on cyber security would be welcome**, particularly given the largely shared threats they face. As part of its recent Cyber Security Strategy, the UK has committed to advancing the UK's global leadership and influence, and collaboration with EU Member States will only serve to further advance progress towards this goal. Additionally, as demonstrated by the 2022 **British-Irish Parliamentary Assembly (BIPA)** European Affairs Committee's inquiry on 'Defence and Security Cooperation Post-Brexit: Cyber Security', there is a clear appetite among the relevant policymakers to ensure there is cooperation between both governments.

To date, the UK has demonstrated some level of cooperation on cyber-related issues with certain EU Member States, such as the Netherlands, however it is evident that the EU and UK have significantly more work to do to develop their collaboration in this regard. As per the 2021 **EU-UK Trade and Cooperation Agreement**, both sides should "endeavour to establish a regular dialogue in order to exchange information about relevant policy developments", as well as crucially share best practices in the area of cybersecurity and protection. As a member of ENISA with strong links to the UK and access to fora such as BIPA, Ireland should be at the forefront of EU-UK cooperation on cyber security, for example by ensuring that any campaigns carried out in coordination with ENISA (e.g. European Cyber Security Month) take steps to involve UK colleagues and ensure alignment with the Trade and Cooperation Agreement.

Citizens

The digitalisation of society must always go hand-in-hand with citizen engagement and involvement in the digitalisation process. This not only means ensuring a certain level of digital literacy, including on cyber issues (as mentioned above), but also ensuring improved access to everyday services for citizens.

A prime example of this is the **'smart city'**, which offers countless benefits for citizens – such as equitable access to connectivity solutions and expanded possibilities for remote work – however this could also open up cities to greater and newer threats, in particular cyber threats. Therefore, it is pivotal that the roll-out of smart solutions in communities occurs alongside the development of secure and resilient digital infrastructure. Additionally, such programmes should be accompanied by extensive **public information campaigns** to inform citizens of potential cyber threats that come from the provision of such services, e.g., the expansion of public Wi-Fi services, and how citizens can ensure such services remain protected from potential cyber-attacks.

Governance Framework and Responsibilities

Cisco welcomes the proposed creation of an **Advisory Group composed of representatives from across the cyber security ecosystem**. This is a crucial opportunity to bring together the wealth of knowledge, both indigenous and Irish-based foreign companies, which has been accumulated over the past few years. Additionally, given the

significant expansion in the size and headcount of the NCSC, such an Advisory Group would act as an excellent forum for an exchange of best practices and discussion on the path forward for Ireland’s cyber strategy up to 2024 and beyond.

Furthermore, given the **developments at an EU level** since the publication of the strategy and the presence of numerous stakeholders operating in multiple EU Member States, such an Advisory Group would provide the **opportunity for industry, academia, etc.** to exchange views on where they see Ireland’s position in the context of the EU’s cybersecurity activities and crucially, how Ireland can further make the most of its position in the EU cyber ecosystem. Cisco is keen to participate in such a forum and looks forward to the call for applications in the near future.


Conclusion

Cisco would like to thank the Department for the opportunity to submit comments to the National Cyber Security Strategy 2019-2024 Mid-Term Review. We would be happy to provide further input to the process at a later stage, as the Department and NCSC’s work programme progresses. Cisco also looks forward to participating in the consultative webinars with relevant stakeholder groups, which the Government intends to host in the coming months.

[Redacted signature block]

Where Cisco can help

As mentioned in the introduction, Cisco possesses a wealth of cyber security expertise drawn from an international network of experts. [Cisco Talos Intelligence Group](#) is one of the largest commercial threat intelligence teams in the world, comprised of world-class researchers, analysts and engineers. The teams are supported by unrivaled telemetry and sophisticated systems to create accurate, rapid and actionable threat intelligence for Cisco customers – both public and private bodies.



Some highlights from the **Cisco Talos Intelligence Group** for Q3 2022 include:

- **Ransomware** continues to be the top observed threat and the top initial access vector was the use of valid credentials, i.e., attackers were using known, valid usernames/passwords to gain access.
- Aligned to this, the top weakness observed by Talos was a **lack of multi-factor authentication**.
- During Q3, **education** was observed as the highest targeted sector, followed by energy, financial services, and Government.

Some statistics on Talos:

- Talos sees **1.4 million** new malware samples per day
- Talos sees **625 billion** web requests per day
- The Talos Vulnerability Research team discover over **200** new vulnerabilities per year

Alongside Talos, this consultation response has noted many other areas where Cisco can help the NCSC improve its **cyber defence strategy that is built on best in class planning, execution and governance**. While we acknowledge that many of these themes may already be activated and actioned to some level of maturity within the NCSC, we have endeavoured to advise based on our knowledge of strategy development and execution in other countries. There are some easy to implement topics which Cisco would like to highlight and may provide some immediate benefits:

Participation in an NCSC Advisory Group

- As outlined in the consultation paper and highlighted above, the NCSC intends to establish high-level fora and/or advisory groups, e.g., the Advisory Group on cyber security. Cisco is keen to engage and share any knowledge, best practices, etc. with regard to cyber security and therefore would welcome the opportunity to actively participate in such groups. As mentioned above, we have extensive experience operating in numerous countries and engaging with national cyber security officials – experience that we believe could be of great utility in establishing such groups in Ireland.
- Through its **Advanced Security Research team**, Cisco has made research grants available to higher education research institutions to drive innovative cybersecurity research that will help mitigate current and future threats. Through collaboration with Cisco customers and researchers, our **Cisco Fellows, Distinguished Engineers and Principal Engineers** have identified a number of key areas, including privacy

and analytics, system integrity, and threat mitigation. When establishing the proposed Advisory Group, the NCSC should explore and engage with such R&D programmes that are already up and running in order to better understand the opportunities and challenges afforded by such programmes. In this regard, Cisco is very willing to share its experiences with such programmes

Vulnerability assessments

- Cisco believes in a holistic approach to vulnerability management; a proactive strategy to identify, track, prioritize, and remediate security weaknesses and flaws in IT systems and software. In recent years, risk-based prioritization has become the gold standard for managing mounting cyber threats against finite resources, allowing providers, such as Cisco to offer **data-driven, predictive analytics based on real-world threat intelligence and business context** to help define the organization’s riskiest vulnerabilities before exploitation occurs.
- [REDACTED]

Supply chain security

- Across our engineering, manufacturing, technical services teams, Cisco manages a coordinated program together with our suppliers and channel partners, to ensure the most effective technology is used to, among other things, limit the introduction of malware and/or rogue components that could compromise functionality across the entire lifecycle of a product.
- [REDACTED]
- [REDACTED]

Development of standards / certification for critical infrastructure providers

- Cisco invests significantly in ensuring that trust and trustworthiness is built into all of our products and services. Measures span our entire development lifecycle including secure development practices, testing, **supply chain and through-life vulnerability management**. In critical national infrastructure, having trust in the underlying technology is key.
- Cisco would welcome the opportunity to collaborate with the Government to explore the development of standards, principles or other guidance that would help set a minimum baseline for network devices used in this sector.

-
- Similarly, Cisco would welcome the opportunity to work with the NCSC to develop the proposed **database of critical infrastructure, vendors, and managed services** as a means of further increasing and optimising the security levels for public and private bodies in Ireland by ensuring trustworthy systems are in place

NIS Directive Audits

- A key step in the protection of national critical infrastructure is assessing the current capability and maturity of existing security installations.
- Cisco are open to discussing how our **CDA program** could be utilised to conduct maturity assessments in key critical infrastructure providers

DNS Protection

- **Cisco Umbrella** is a global secure Internet DNS platform which is designed to prevent access to malicious sites based on their DNS name.
- The platform processes in excess of 170 billion DNS queries daily which provides a unique insight into the global threat landscape ensuring that customers can be provided with rapid protection from malicious sites.



Engagement

As a multinational company, Cisco are engaged on the topic of cybersecurity in countries across the globe including the UK, **France, Italy, Germany, Australia, India and Singapore**. In each of these regions, Cisco helps to support a broad spectrum of cyber initiatives ranging from skills and education programs, cyber policy development and formal assurance and certification efforts.

We have also engaged with key stakeholders at the EU level on the EU Cybersecurity Certification, the European Cyber Resilience Act, and the Network and Information Security (NIS) Directive 2.

Skills

- As noted in the consultation paper, Cisco has been working with the Department on Skills and are keen to continue and deepen such a collaboration, in particular with regards to upskilling and reskilling for cyber.
- Through its **Networking Academy (NetAcad)**, Cisco offers online and in-person training for 3.2 million enrolled students globally, with courses on cybersecurity among the core subjects covered in the online courses with modules cloud security, IoT security, and cybersecurity essentials. In the coming months, Cisco hopes to expand the availability of such courses to both students and employees through reskilling, upskilling, apprenticeships and other training programmes – including for SMEs.