Oibríochtaí Gnó, Foireann AD rShláinte agus Teicneolaíocht Bhunathraitheach,

FSS, Ospidéal Dr. Steeven's,
Baile Átha Cliath 8, D08 W2A8

eHealth and Disruptive Technologies

HSE, Dr. Steeven's Hospital,
Dublin 8, D08 W2A8

27/01/2023

Dear [redacted]

Thank you for providing the HSE with the opportunity to input on your consultation paper on the National Cyber Security Strategy.

On behalf of the HSE, eHealth, and the Office of the CISO we have attached a number of observations which may be of help as you undertake your mid-cycle Strategy Review. Should you wish to discuss any of the observations further please feel free to reach to us at your convenience.

Yours sincerely,

[redacted]

[redacted]
Delivery Director
Cyber Security Strategy & Information Security
FSS |Ospidéal Dr. Steevens|Baile Átha Cliath 8 | D08 W2A8
HSE| Dr. Steevens' Hospital |Dublin 8|D08 W2A8|

[redacted] | ☎: +[redacted] | www.hse.ie

Oibríochtaí Gnó, Foireann AD rShláinte agus Teicneolaíocht Bhunathraitheach,

FSS, Ospidéal Dr. Steeven's,
Baile Átha Cliath 8, D08 W2A8

eHealth and Disruptive Technologies

HSE, Dr. Steeven's Hospital,
Dublin 8, D08 W2A8

Feedback - NCSC mid-term Strategic Review

1. There needs to be a recommendation on how such additional requirements will be funded, as investment cyber funding will be a key enabler for success.
2. The end-state is not a closed loop and ongoing investment support needs to be called out to help the ongoing demand for growth in capabilities.
3. The criteria for success and compliance is not clearly defined in the strategy.
4. Clearly defined deliverables from ENISA need to be articulated with practical and achievable timelines for state bodies.
5. No sample organisational structures have been recommended that will help shape CISO organisational structures across government agencies, that align at a national level.
6. There needs to be a clear specification for national shaped Cyber Risk Management with aligned specifications with the NIST Directive, including Cyber Risk Management, CSIRT, Cyber Defence and Cyber Platform Management.
7. More regular Threat Infographics should be part of the centre's strategic deliverables.
8. The establishment of an out of hours, full 24x7 early warning service would prove beneficial, the communication capabilities with the current service is inadequate.
9. Uniform engagement should be extended beyond Public Sector to include 3rd parties supplying services to all Public Sector bodies and an equal spread of the collective security burden.
10. The strategy needs to embrace awareness of the commercial reality of the burden of cyber security and help with supporting judgement on providing the right level of investment versus risk for senior decision makers.
11. The NCSC strategy should include an effective way to incentivise adoption across both the public and private sectors seeking a widespread and uniform implementation of Secure by Design.
12. The strategy should give consideration to greater regulation and other tools and frameworks to address the transformation needed.
13. The strategy should give consideration to supply-chain risks and the capability to assess manipulative software and technologies.
14. The strategy should give more detailed focus on cyber innovation centres which can be leveraged at short notice by both public and private sector bodies alike.
15. There is a need to ensure the strategy comprehensively captures the relevant principles of the GDPR Regulation including security by design and data protection.
16. The strategy could benefit from a stronger focus on the security dimensions of cloud computing which represent a large growth area