Feidhmeannas Seirbhíse Sláinte
Health Service Executive

Office of the Chief Information Officer
delivering eHealth Ireland,
Dr. Steevens' Hospital
Steevens' Lane
Dublin 8

Ph: 01 635 2732
Fax: 01 635 2740

22nd September 2021

Mr. Neale Richmond TD
Dáil Eireann
Leinster House
Dublin 2

Re: PQ ref 43058/21

''To ask the Minister for Health the work he has undertaken to address cyber-security measures faced by the Health Service Executive to prevent further cyber-attacks; and if he will make a statement on the matter.''

Dear Deputy Richmond,

The HSE places great importance on the criticality, integrity and availability of services and information required to protect the health and well-being of service users. This is central to the strategy of the organisation and is supported by policies and procedures, with appropriate controls in place. Aligned with the HSE strategy is a technology strategy which is underpinned by IT General Controls to mitigate Information Security Risk to the organisation.

The HSE continues to improve the Cyber Security Risk posture through:

- Development of a security organisation, including 24X7 Security Operations Centre.
- Investment in key security technologies/controls.
- Modernisation of technology foundation.
- Increasing Cyber Security Awareness at all levels of the organisation.
- Alignment with the NIST framework for the management of security, initial focus OES Systems.

Following the cyber-attack the HSE had implemented a number of enhancements across the domain. These include additional tool sets and Cyber Security experts suggested improved configuration profiles to our servers. The range of improvements include the following.

Additional Cyber initiative undertaken since the Cyber Breach

Risk Area	Post Cyber Enhancement
Cyber Security Services	Cyber Security Experts Remediation and Investigation Services
Cyber Security Services	All domain servers have been subject to Cyber Security Experts recommended Cyber Hardening
Cyber Security Services	Multi factor authentication for all remote access
Cyber Security Services	24x7 Enhanced Security Operations – (Anti-Virus)
Cyber Security Services	24X7 Cyber Security Defence Monitoring
Cyber Security Services	24x7 Cloud Security Monitoring Services
Control – Endpoint Protection	Additional vendor providing endpoint protecting
Control – Endpoint Protection	Network endpoint network access control pilot
Control – Network Monitor	Network egress monitoring and detection
Control – Endpoint Protection	Government Network and HSE DNS monitoring

Please see Appendix A below for summary of approach and activity.

If you feel that the question has not been fully answered or you require any further clarity, please contact me.

Yours sincerely,

Fran Thompson,
Interim Chief Information Officer, OoCIO, HSE.

Appendix A: - HSE Cyber Security Risk Management Approach & Control Improvement Activity

Cyber Security Management - Key Risk Factors

1. Cyber Security Investment – technology and resources.
2. Cyber Security Awareness Management.
3. Cyber Security Control Environment.
    a. Asset Management linked to Service Criticality.
    b. Software Currency - Extent of legacy infrastructure, patching programme.
    c. Access management, with focus on privileged access, authentication controls.
    d. Protection controls, endpoint protection, perimeter protection.
4. Cyber Security Governance (including risk management).
    a. Enterprise Risk – aligned with HSE Integrated Risk Management Policy.
    b. Board Awareness.
    c. Compliance (including Audit).

Risk Area	Cyber Security Programme Activity	Status	2019	2020	2021	2022	2023	2024	2025
Cyber Security Control									
Control - Asset Management	Criticality List - OES	100%							
Control - Asset Management	Criticality List - Beyond OES	80%							
Control - Asset Management	Criticality List - Technology Vendors	100%							
Control - Asset Management	Application Inventory	80%							
Control - Asset Management	Infrastructure Inventory	90%							
Control - eMail Hygiene	eMail Filtering, Anti-Spam (TopSec)	100%							
Control - eMail Hygiene	eMail Filtering Sandbox Environment (TopSec)	100%							
Control - eMail Hygiene	eMail Phishing Protection/Awarenes s (MXToolbox)	100%							
Control - eMail Hygiene	eMail SPAM Blacklist (SPAMHAUS)	100%							
Control - Endpoint Protection	End Point Protection - McAfee enhancement	100%							
Control - Endpoint Protection	End Point Protection - Cylance Pilot	100%							
Control - Endpoint Protection	Enterprise Patch Management Tool	100%							
Control - IAM	Multi-factor authentication - Risk based approach	WIP							
Control - Legacy	Windows Server & SQL Server Upgrades	90%							

Risk Area	Cyber Security Programme Activity	Status	2019	2020	2021	2022	2023	2024	2025
Control - Legacy	Windows 7 Upgrade Programme	50%							
Control - Legacy	VMWare & Citrix	100%							
Control - Legacy	Network & Communications	93%							
Control - Legacy	Privilege Access Review	WIP							
Control - Strategy	Cloud Deployments	WIP							
Control - Strategy	Consolidation of all identities into a single platform HealthIRL.	60%							
Control - Strategy	Platform consolidation.	Continuous							
Control - Strategy	Cloud Identity	90%							
Control - Strategy	Role Based Access - Initial target Account Management Processes	Continuous							
Control Audit	Outstanding Audit actions - 2018 (44%), 2019 (10%), 2020 (< 5%)	Continuous							
Cyber Security Awareness									
Cyber Security Awareness	Ongoing awareness campaigns: #ThinkB4UClick.	Continuous							
Cyber Security Awareness	Focussed communications.	Continuous							
Cyber Security Awareness	Critical services known and understood.	100%							
Cyber Security Awareness	Participation in NIS Directive as an Operator of Essential Services.	Continuous							
Cyber Security Awareness	Member of the National Strategic Emergency Management critical infrastructure resilience review.	Continuous							
Cyber Security Awareness	Cyber Security Board Presentation	Continuous							
Cyber Security Awareness	elearning Cyber Security Awareness Staff Training Platform	95%							
Cyber Security Governance									

Risk Area	Cyber Security Programme Activity	Status	2019	2020	2021	2022	2023	2024	2025
Governance	Adapt Cyber Security Control Framework - NIST	WIP							
Governance	Align with HSE Integrated Risk Management Policy	Continuous							
Governance	HSE Security Policy Enhancement - updates to current, development of new in line with strategy	WIP			October				