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

21st September 2021

Mr. Brendan Griffin TD
Dáil Eireann
Leinster House
Dublin 2

Re: PQ ref 41879/21

''To ask the Minister for Health the total amount spent to date by the HSE in rebuilding systems after the cyber-attack; and if he will make a statement on the matter.''

Dear Deputy Griffin,

The Health Service Executive (HSE) has been requested to reply directly to you in the context of the above Parliamentary Question, which was submitted to the Minister for Health for response.
I have reviewed that matter and the following composite reply is the current position.

On 14th May 2021, the HSE became aware of a significant attack on some of its ICT systems. In the early hours of Friday morning, 4am, the on-call critical incident co-ordinator escalated the matter based on several instances of malware being identified. Having assessed the scale of the threat, the level of risk, the type of malware detected and the impacted environment it became apparent that this was a major and a sophisticated attack.

The cyber-attack against the HSE's ICT infrastructure has been significant and unprecedented in severity and scale. The identified expected centrally incurred costs of up to €99m (€30m once-off + €69m recurring) which will be spent in 2021 and 2022.

The expenditure to date by the HSE totals 10.46m.

This expenditure to date relates to vendor support and external strategic partners. These vendors and strategic partners were brought on board to support the HSE in rebuilding the servers and applications to fully restore and improve where possible the systems.

Vendor support has enabled an accelerated implementation of an interim Security Operations Centre (SOC) which continuously monitors and identifies potential threats to our Servers and

Hardware. Other supporting measures include the initiation of a roll-out of MFA (Multi Factor Authentication) across the organisation and provision of a managed security service via Mandiant/FireEye, which includes continuous monitoring and protection across all HSE devices daily.

The HSE's External Strategic Partners have been able to advise on leading cyber security strategy which utilises Artificial Intelligence (AI) and Security Orchestration Automation and Response (SOAR) technologies to focus' on three critical areas: speed of detection, response, and recovery with a focus on improvement in cyber operational technology (OT) resiliency.

The consolidation and investment in critical infrastructure and information capabilities, ensures that security is at the core of system development and improvement planning and in the recovery transformation. The successful delivery of protected systems and infrastructure will improve day to day operations across our hospital network to safely manage services in real time.

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.