



Príomhoifigeach Faisnéise

rShláinte agus Teicneolaíocht
Bhunathraitheach FSS, Ospidéal Dr
Steevens, Baile Átha Cliath 8, D08

Chief Information Officer

eHealth and Disruptive Technologies,
HSE, Dr. Steevens' Hospital, Dublin
8, D08 W2A8

www.hse.ie

ehealthireland.ie
[@hselive](https://twitter.com/hselive)

t 01 635 2732

8th April 2022

Mr. David Cullinane TD
Dáil Eireann
Leinster House
Dublin 2

Re: PQ ref 16536/22

“To ask the Minister for Health the range of hospital equipment which may need to be replaced or upgraded to protect the health system from a cyber-attack; and if he will make a statement on the matter.”

Dear Deputy Cullinane,

Cyber Security risk posture from an infrastructure (equipment) perspective is dependent on two aspects:

1. Security & Currency of foundational technologies – devices, servers, networks, applications.
2. Specific Cyber Security Technologies which detect and protect services from Cyber Attack.

As part of the Capital Plan 2022, the HSE has allocated €59.8 million on Foundational Infrastructure and Cyber Technologies. The table below shows a broad break down of the spending within the categories.

Category	Capital Programme		2022
1. Foundational Infrastructure & Cyber Technology	1.1	Network & Communications Technologies	€7,650,000
	1.2	Refresh Current Technology & Devices	€24,709,110
	1.3	Single Identity	€5,100,000
	1.4	Data Centre & Cloud Services	€6,120,000
	1.6	Cyber Security Technology	€11,150,000
	1.7	New Technology	€5,100,000
		Subtotal	€59,829,110



Security & Currency of Foundational Technologies – planned spend €35m.

The HSE had an existing refresh programme for foundational technology prior to the cyber-attack. Following on from the attack this programme has been accelerated and prioritised. Included in the refresh programme spend are end user devices, legacy servers and network technologies; the replacement of these would improve the cyber posture of the organisation. There are also programmes of work addressing legacy applications in hospital environments.

Cyber Security Technology – planned spend €11m.

In response to the cyber-attack the HSE has expanded, accelerated and prioritised the existing Cyber Security Technology improvement programme. This programme is implementing new security technology for the detection and protection against Cyber Attack. The HSE has also augmented their security operations management. The combination of the security technology solutions and security operations mitigate cyber security threat as the refresh programmes continue to deliver.

Note: The total €59m figure includes capital for new services, capacity demands and BAU operations.

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

Yours sincerely,

A handwritten signature in blue ink that reads 'Fran Thompson'.

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