Response to “A call for views – Australia’s 2020 Cyber Security Strategy

11. What specific market incentives or regulatory changes should Government consider?

With healthcare undergoing digital transformation, there is an increase in the adoption of connected medical devices. From a cyber security perspective, it is a challenge to be able to complete security assessments in a timely manner due to the rate of adoption and the diversity of connected medical devices. Not to mention, it can be assumed that there is significant duplication in effort nationally from healthcare providers in performing similar assessments.

Whilst there is a cyber security guidance document for the medical device industry, further clarity will need to be provided on the manufacturers’ responsibility for ensuring their medical devices are cyber secure. Availability of a security compliance measure will also assist with purchasing decisions and reduce the duplicated effort from performing standalone security assessments.

12. What needs to be done so that cyber security is ‘built in’ to digital goods and services?

Whilst the need for a ‘trusted market’ of secure technologies, products, services and professionals is being recognised as being critical for improve cyber security outcomes in Australia, the underlying processes to procure technologies and services needs to be reviewed to ensure procurement is achieved in a timely manner balancing against the rate of change in technology. National facilitation of cyber security technology adoption will assist with streamlining procurement decisions.

14. How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?

With the high demand for skilled cyber security professionals, the government sector is competing against the private sector for the same pool of talent. Advancement pathways that differs to the traditional management path within the government sector needs to be considered to retain and attract talent.

It is also important to recognise that there is demand in regional areas for cyber security professionals as digital transformation has removed the traditional geographical barriers, more needs to be done to provide cyber security support to services operating in regional areas.

19. What private networks should be considered critical systems that need stronger cyber defences?

Further clarity and consistency on whether the health sector is considered critical infrastructure from a cyber security perspective is required.