

Samuel Grunhard  
First Assistant Secretary  
Critical Infrastructure Security  
Department of Home Affairs  
By email to CI.REFORMS@homeaffairs.gov.au

Copy to Professor Brendan Murphy  
Secretary, Department of Health

27 November 2020

Dear Mr Grunhard,

### **Protecting Critical Infrastructure and Systems of National Significance**

Thank you for the opportunity to participate in consultation on reforms to protect Critical Infrastructure and Systems of National Significance. Telstra Health appreciates being able to provide a further response to our submission on 15 September, and in addition to our participation in consultation sessions.

The Consultation Paper on Protecting Australia's Critical Infrastructure and Systems of National Significance envisages an extension of the coverage of the critical infrastructure obligations to cover the Health sector. In principle, this extension is supported given the fundamental importance of the health sector to the livelihoods of all Australians.

As we highlighted in our initial response, for such reform to be effective and practically workable, it must be founded on a clear understanding of the multi-jurisdictional, public, private and community-based structure of Australia's health system, as well as its funding and information flows.

We welcome the increased specificity set out in the Exposure Draft and Explanatory Document, although we repeat our advice that the interconnected nature of health service delivery may mean that the intent of the measures may be difficult to achieve due to the complex supply lines relating to hospital care in particular. We recommend active, ongoing industry collaboration to address this matter.

This submission seeks clarification of some specific measures, and reiterates the need for clear, principle-based guidance to support the intended outcomes in the health sector.

### **Anticipated impact on Telstra Health as a health technology provider**

In the current form of the proposals, we understand the likely coverage and impact for Telstra Health to be:

- Subject to Government Assistance measures as a part of the economy that involves the production, *distribution and supply of medical supplies*- in that some health software is classified as a medical device and therefore a therapeutic good under the TGA regulations.

- As a technology supplier to *critical hospitals* operating Intensive Care Units that would be captured as Critical Infrastructure Assets, and required to fulfill Positive Security Obligations as well as Government Assistance measures. Telstra Health is a supplier of health software to public and private hospitals that operate Intensive Care Units, including specific ICU clinical software in some cases.
- We understand that health assets are not envisaged to be captured in the definition of Systems of National Significance.

### **Seeking clarification of coverage for digital health infrastructure**

Telstra Health operates jurisdiction-wide population health data on behalf of governments, including the National Cancer Screening Register, and Real Time Prescription Monitoring systems (through our joint venture Fred IT). These systems are underpinned by enabling legislation that sets out robust governance overseen by relevant Government Departments and Ministers.

We had not expected any additional security measures or reporting obligations above those already required under this existing legislation- and indeed the Explanatory Document appears to echo this sentiment when it sets out that *“Digital infrastructure has not been captured as the Government has robust safeguards implemented around control and access defined within legislation such as the My Health Records Act 2012. The Government is responsible for a large portion of the digital infrastructure that supports the health sector.”*<sup>1</sup>.

However, the relevant provision in the Bill exempts such systems from being classified as critical infrastructure asserts on the basis of being ‘owned’ by the Commonwealth, which is distinct from operational accountability for systems owned by third party suppliers.

We ask for clarification whether the intent is to exempt all digital health infrastructure that is already subject to similar legislative requirements, and/ or whether other systems such as the NCSR and RTPM may be specified as exempt in the relevant Rule.

### **Challenges with effectiveness compliance in the health sector**

To echo our advice in our submission in August, healthcare is characterised by interwoven layers of governance, regulatory and operational responsibilities. The majority of health services and health infrastructure providers are wholly or substantially government funded, either on a fee-for-service basis, contractually, or through state public health services directly funded by government. States and Territories deliver public hospital services (though not under uniform governance models), and private hospital groups have an increasing role in healthcare delivery.

Technology and people-based systems that are relevant to security and continuity of service in healthcare are interconnected, not necessarily governed by aligned frameworks, and certainly subject to long and complex supply chains.

---

<sup>1</sup> Explanatory Document paragraph 168, p29.

Therefore, the ability for a *critical hospital* to completely control for risk in this environment is challenging. This has a bearing on the practicality of implementation, as well as the cost implication of compliance- in that the actions and costs may relate not only to the regulated entity, but potentially to third parties in the supply chain including health software providers, or other parties within the clinical delivery ecosystem.

#### The need for clear principles-based guidance

Considering the policy and operational interrelationships in the sector, Telstra Health recommends the incoming reforms and guidance provide sufficient clarity for providers operating in this complex policy and service delivery environment. Healthcare providers will benefit from clarity of:

- The nature of real-world threats and impacts on ‘social and economic’ factors;
- How organisations and operators should treat supply chains and co-dependent organisations in light of the Critical Infrastructure requirements; and
- The respective security obligations under SOCI, Privacy and My Health Record Acts.

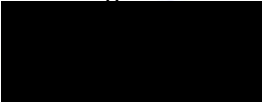
Telstra Health encourages the Department to explore and account for these issues, in order that requirements for health are appropriate, including:

- Appropriate sector specific definitions of Critical Infrastructure Assets and Systems of National Significance (SONS);
- Appropriate materiality thresholds for mandatory incident reporting and other reporting requirements;
- Government Assistance interventions that are directly responsive to identified threats, noting the diversity of entities and roles in health delivery- even within a single patient episode;
- Appropriate guidelines in relation to security obligations that will apply to supply chains; and
- Ensuring that sector specific standards are fit for purpose and do not impose unnecessary or unreasonable costs of compliance on industry.

#### **Working with the Department going forward**

Telstra Health is Australia’s largest provider of digital health solutions and a wholly owned subsidiary of Telstra Corporation, who has also made a response to this consultation. The Telstra Health team and I are happy to collaborate with the Department on any of the issues raised in this submission, and on development of health sector standards relating to these reforms.

Kind regards



Graeme Osborne  
Head of Hospitals and Connected Health  
Telstra Health

[Click here to enter text.](#)