Samuel Grunhard
First Assistant Secretary
Critical Infrastructure Security
Department of Home Affairs

By email to CI.REFORMS@homeaffairs.gov.au

Copy to
Dr Brendan Murphy
Secretary, Department of Health

15 September 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 formal response to the proposals put forward, supplementary to our participation in Health Sector workshops in August.

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 which has been brought to the fore at this time.

However, 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.

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 supplier and operator of **Critical Infrastructure Assets** in health- defined as *assets, systems or networks involved in the provision of health care, production of medical supplies and medical research*, in that:
  - Telstra Health supplies health software and digital connectivity to public and private hospitals, aged care, indigenous primary health, disability care, and telehealth services across Australia- as well as community pharmacy systems and a Prescription Exchange Service through our joint venture Fred IT.
  - Telstra Health also manages 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). We do not expect any additional security measures or reporting obligations above those already required under existing legislation and governance relating to these systems.
- As a supplier to hospitals operating Intensive Care Units that would be captured as **Regulated Critical Infrastructure Assets,** and required to fulfill Positive Security Obligations as well as Government Assistance measures, in that:
  - Telstra Health as 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**.

- We are happy to advise and participate in codesign of sector-specific standards for health entities.

Understanding the health sector context

The social and economic impact of the current pandemic may increase awareness for Home Affairs to consider health services in the Critical Infrastructure context. In addition to responding to questions put by the Consultation Paper (provided below), Telstra Health offers the following advice in order that the legislative reforms and subordinate instruments and guidance might both meet the stated objectives and be fit for purpose in health settings in Australia:

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.

In primary care, general medical practice (GPs) and pharmacy are private businesses. It should also be noted that under the Constitution, doctors cannot be civilly conscripted.

Aboriginal Medical Services are a mix of Commonwealth, state and territory and community-controlled models. Aged care is also a mix of government and private funding arrangements- largely privately provided, but with strong government regulation.

The strongest existing national data governance framework for Health is the Commonwealth Privacy Act, generally echoed in State privacy legislation, and there are security and related reporting obligations under the My Health Records Act for providers and software vendors that connect to that system. State and Territory legislation also governs the structure and operation of health services and has a bearing on physical, cyber, personal and supply chain security, and applies across a diverse range of physical settings and clinical modalities. Further, professional bodies have a role in setting appropriateness of security measures in clinical settings, such as Royal Australian College of General Practitioners (RACGP) *Computer and Information Security Standards*.

The Commonwealth does not directly deliver health services, though has a regulatory role exercised through funding and accreditation mechanisms. As such, there is no Commonwealth health legislation or policy framework that is a natural home for sector-wide security obligations across all relevant jurisdictions and commercial settings.

Technology and people-based systems that are relevant to continuity of service in healthcare are interconnected and not necessarily governed by aligned frameworks. Therefore, the actions, controls and declarations of any one entity may not align with the scope of issues identified by Home Affairs as nationally significant.

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;
- Definition of services, including reuse of definitions from relevant legislative instruments where possible;
- How organisations and operators should treat supply chains and co-dependent organisations in light of the Critical Infrastructure requirements; and
- The interrelationship with security obligations under 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 Regulated Critical Infrastructure Entities 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 have also made a response to this consultation. The 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

[redacted]

Professor Mary Foley AM

Managing Director

Telstra Health

Telstra Health Submission to consultation questions

Overall Framework

Telstra's Health's response to the "call for views" made by the Government are as follows. Note also that Telstra Corporation has also made a separate response to this consultation.

#	"Call for views"	Response
1	Do the sectors above[1] capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?	*No response*
2	Do you think current definition of Critical Infrastructure is still fit for purpose?	Telstra Health agrees that the proposal to include health assets may satisfy the criteria under Section 9(3), in the ability to identify and respond to threats to essential health services, and to population wide health threats has an impact on social and economic stability. We suggest any broad definition of 'health' align with other legislative definitions: • as 'health service' under the Commonwealth Privacy Act 1988; • 'hospital service' as defined under the Health Insurance Act 1973; • National Health Act refers to the definition of 'public hospital' made under the Private Health Insurance Act 2007.
3	Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?	*No response*
4	What are the common threats you routinely prepare for and those you have faced/experienced as a business?	Telstra Health provides health software to a variety of healthcare providers, and to jurisdiction-wide platforms for government, and so threats vary across these settings. The principal threats to health software are: • Malware (software written with the intent to damage, exploit, or disable devices, systems, and networks. Incursions which include but are not limited to Malware, Ransomware, Distributed Denial of Service (DDOS)). • Transmission failure due to failure or compromise of physical asset

[1] • Banking and finance • Communications • Data and the Cloud • Defence industry • Education, research and innovation • Energy • Food and grocery • Health • Space • Transport • Water

#	"Call for views"	Response
		• Social engineering • Patch management • BYOD management • Cloud vulnerabilities
5	How should criticality be assessed to ensure the most important entities are covered by the framework?	The nature of criticality will change over time and context. Telstra Health argues that threat and impact assessment should be made by operators and existing governance, informed by external guidance and review.
6	Which entities would you expect to be owners and operators of systems of national significance? **Additional Question:** Should owners and operators be subject to the same requirements?	*No response; Telstra Health understands that Health assets are not being considered as SONS.*

Industry collaboration to support uplift

#	"Call for views"	Response
7	How do you think a revised Trusted Information Sharing Network for Critical Infrastructure (**TISN**) and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?	*No response.*
8	What might this new TISN model look like, and what entities should be included?	*No response.*
9	How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus? **Additional Question:** What should be Government responsibility and what should be the responsibility of industry in this relationship?	*No response.*

Initiative 1 – Positive Security Obligation

Telstra Health's response to the "call for views" made by the Government are as follows:

#	"Call for views"	Response
10	Are the principles sufficiently broad to consider all aspects of security risk across sectors you are familiar with?	Yes the principles are sufficiently broad to capture threats in health settings.
11	Do you think the security requirements strike the best balance between providing clear expectations and the ability to customise for sectoral needs?	Without visibility of specific legislative provisions, and guidance, it is not possible to determine the appropriateness of requirements on the health sector.

#	"Call for views"	Response
12	Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles? **Additional Question:** Please outline what Telstra is currently doing in relation to each principle. **Additional Question:** What physical security measures has Telstra recently introduced in response to physical incident issues? **Additional Question:** What cyber security protections are in place to protect Telstra's systems and information from cyber threats? **Additional Question:** What supply chain protections are currently in place?	There is diversity in formal requirements and practices across health care settings, and Telstra Health does not have a view on sector behaviour regarding security requirements necessary for Regulated CI services.
13	What costs would organisations take on to meet these new obligations?	Estimates of costs will depend on final definition and scope of CI in Health. Without visibility of specific legislative provisions, and guidance, it is not possible to determine the costs of obligations on the Health sector. Note that 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.
14	Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what? **Additional Question:** How should the new framework interact with the TSSR?	The Commonwealth Privacy Act 1988 provides the strongest national framework for data governance and security (generally echoed in State privacy legislation) but does not address continuity of service that may be more relevant to the CI Reforms. There are also security and related reporting obligations under the My Health Records Act for providers and software vendors that connect to that system. *Note that Telstra Corporation has provided a response to the additional question posed.*
15	Would the proposed regulatory model avoid duplication with existing oversight requirements?	The strongest existing data governance framework for Health is the Commonwealth Privacy Act, generally echoed in State privacy legislation, and there are security and related reporting obligations under the My Health Records Act for providers and software vendors that connect to that system. State and territory legislation also governs the structure and operation of health services and has a bearing on physical, cyber, personal and supply chain security, and applies across a diverse range of physical settings and clinical modalities.

#	"Call for views"	Response
16	The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?	Subordinate instruments and guidance should make specific reference obligations and definitions under existing data governance and other security legislation in place at Commonwealth, jurisdictional levels, and under profession-specific guidelines. It should also address obligations as they apply across sectors, noting the interdependency between health, data services, and utility infrastructure providers. The reforms should introduce appropriate protections to ensure that a single perceived or actual failure to comply with the obligations is not considered to be a separate failure in each sector. The incoming reforms and guidance must provide sufficient clarity for providers operating in a 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; • Definition of services, including reuse of definitions from relevant legislative instruments where possible; • How organisations and operators should treat supply chains and co-dependent organisations in light of the CI requirements; • the interrelationship with security obligations under Privacy and My Health Record Acts; and • the interrelationships and dependencies in other sectors.
17	Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?	There is no Commonwealth health legislation or policy framework that is a natural home for sector-wide security obligations across all relevant health jurisdictions and commercial settings.
18	What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?	*No response*
19	How can Government better support critical infrastructure in managing their security risks?	We recommend that the following support be provided: • Regular threat briefings, relevant information sharing. • Clear, concise, timely, scenario-specific advice that is easy to share with relevant specialist teams e.g. software developers, implementations teams, procurement, finance.

#	"Call for views"	Response
20	In the AusCheck scheme potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?	Telstra Health does not use the AUSCHECK program. Rather, we use the DISP system conducted by Defence and as directed by the Department of Health as a requirement for our role in operating the National Cancer Screening Register (NCSR). The NCSR is ISM compliant and governed by the Commonwealth NCSR Act.
21	Do you have any other comments you would like to make regarding the PSO?	*No response*

Initiative 2 – Enhanced Cyber Security Obligations

Telstra Health understands that no health assets, systems or organisations are being considered as SONS. We therefore do not offer a response to questions 22-28.

Telstra Health's response to the "call for views" made by the Government are as follows:

#	"Call for views"	Response
22	Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities? **Additional question:** What is your view of the proposed cyber security activities?	*No response*
23	What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing? **Additional Question:** How can the Government effectively share aggregated threat information? Is there an existing process that works well?	*No response*
24	What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?	*No response*
25	What methods should be involved to identify vulnerabilities at the perimeter of critical networks?	*No response*
26	What are the barriers to owners and operators acting on information alerts from Government?	*No response*
27	What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?	*No response*
28	What safeguards or assurances would you expect to see for information provided to Government?	*No response*

Initiative 3 – Cyber Assistance for Entities

Telstra Health understands that under the current proposals, we would be subject to Government Assistance measures as a supplier and operator of **Critical Infrastructure Assets** in health- defined as *assets, systems or networks involved in the provision of health care, production of medical supplies and medical research*, in that:

- Telstra Health supplies health software and digital connectivity to public and private hospitals, aged care, indigenous primary health, disability care, and telehealth services across Australia- as well as community pharmacy systems and a Prescription Exchange Service through our joint venture Fred IT.
- Telstra Health also supplies 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). We do not expect any additional security measures or reporting obligations above those already required under existing legislation and governance relating to these systems.

With regard to assistance measures, it is essential that appropriate safeguards will be put in place. There should be appropriate protections for (a) information that may be accessed as a result of the Government assistance powers and (b) any contractual liabilities or consequences arising as a result of Government assistance incorporated into the reforms. This should include clear limits and a legal framework that sets out when and for how long the Government can provide assistance to an entity. This framework should also embed consultation as part of the required process.

Cost recovery should be available for entities in certain circumstances, particularly where costs are incurred due to Government intervention. We recommend that entities should have immunity from any liability arising from actions taken in accordance with Government directions or otherwise arising from Government intervention, including for contractual liability for suppliers and customers affected.

Subject to appropriate safeguards being in place, in principle, we agree that Government should have the power to issue reasonable and proportionate directions to entities to ensure that action is taken to minimise the impact of imminent cyber threats or incidents.

Telstra Health's response to the "call for views" made by the Government are as follows:

#	"Call for views"	Response
29	In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?	We anticipate that the Commonwealth Health Minister and Chief Medical Officer would have a prevailing opinion as to the impact an emergent threat, informed by States and Territories as entities responsible for health service provision and continuity.
30	Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first? **Additional Question:** What other basis must there be for an emergency to be declared?	We anticipate that the Commonwealth Health Minister and Chief Medical Officer would have a prevailing opinion as to the extremity of an emergent threat, informed by States and Territories as entities responsible for health service provision and continuity.

#	"Call for views"	Response
31	Who should oversee the Government's use of these powers?	*No response*
32	If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber attack, do you think there should be different actions for attackers depending on their location?	*No response*
33	What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?	*No response*
34	What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?	*No response*
35	What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?	As suppliers to regulated entities, it is critical that those entities have absolute clarity of the nature and rationale for security measure and related reporting requirements. Depending on the setting, there may be additional costs and requirements on suppliers, over and above agreed contractual requirements.
36	Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?	Telstra Heath will be pleased to engage on this question once legislative parameters and subordinate instruments are defined.