NATIONAL COMMITTEE FOR
INFORMATION AND COMMUNICATION SCIENCES

Australian Academy of Science

The National Committee for Information and Communication Sciences of the Australian Academy of Science welcomes the opportunity to comment on the Department of Home Affairs' Consultation Paper on the protection of critical infrastructure. The committee has responded to specific calls for views in the consultation paper, numbered below.

If you would like to discuss any of these matters further, please contact the chair of the committee, Professor Shazia Shadiq ([redacted]), or the Australian Academy of Science via Meaghan Dzundza, Manager National Committees for Science ([redacted]).

Calls for views:

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?

The definitions and factors are quite abstract, and the mapping process at the sector level will need further consultation. The current definitions and factors may create issues for 'micro-entities' being left behind, for example, Internet of Things networks that individually may not fit the definition of 'critical', but collectively could have serious implications for critical infrastructure.

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?

No, a significant journey can be expected before the security obligations are realised in terms of skill shortages, financial burden and time delays.

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?

The importance of domain experts within the regulators for each sector should be recognised, such as security in the higher education sector versus food security.

22: Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?

Establishing a national pool of qualified cyber security experts would assist in this activity.

The Notifiable Data Breach Scheme currently mandates organisations that have experienced data breaches to notify authorities about the breach. The legal penalties currently focus on penalising organisations for not informing about the breach, but not for the breach itself. Organisations hosting critical infrastructure and systems should be liable for a high level of information assurance and should be held accountable in a legal way. This will encourage boards and senior executives to put cyber security on the agenda, and recognise cyber risks as business risks.

Cloud service providers that host services that store/process sensitive data of Australian citizens/residents or hosting services should be able to provide the Australian government and people full transparency about the provenance of data, the locations the data will be stored at and accessed from, and should have high accountability and auditability.