Australian Gas Infrastructure Group

Australian Gas Infrastructure Group
L6, 400 King William Street
Adelaide, SA 5000 Australia
PO Box 6468, Halifax Street,
SA 5000 Australia
+61 8 8227 1500
info@agig.com.au
agig.com.au

16 September 2020

Department of Home Affairs
email: ci.reforms@homeaffairs.gov.au

Protecting critical infrastructure and systems of national significance.

We appreciate the opportunity to provide feedback on the consultation paper Protecting critical infrastructure and systems of national significance. We have welcomed the positive interactions as part of the consultation process, and have provided our feedback in those sessions.

However, as a high-level summary of our views, we recommend:

- Embedding a risk-based approach to managing security risk for critical infrastructure
- Defining the scope of the regulatory regime to only capture the assets and systems for which unauthorised access poses a national security risk. That is, the assets and systems that monitor and control electrified assets (i.e. our operational technology)
- Leveraging existing industry security frameworks to minimise duplication and undue cost, as well as ensuring consistency in frameworks across jurisdictions and consistency of definitions across legislative instruments. Adoption of ISO270001 and the maturity model under AEMO's AESCSF would be appropriate. Establishing standards / guidance for implementing ACSC's Essential Eight Strategies to Mitigate Cyber Security Incidents specific to ICS / SCADA /OT environments would also be appropriate
- Ensuring the compliance and enforcement regime reflects the risk-based framework
- Consideration of the government providing a centralised threat intelligence service through the collection and timely dissemination of actionable information on threats or incidents relating to critical infrastructure
- Consideration of the ASCS role as an intermediary to mitigate supply chain risks, ensuring there is proper segregation, controls, testing and auditing in place end-to-end
- Very carefully prescribing and limiting the circumstances in which government may make directions or take actions to control critical infrastructure and ensure any proposed action are properly consulted and communicated.
- Assisting critical infrastructure providers with selection of the most appropriate toolsets in place to manage cyber security risks. Consistency across providers would be helpful.
- Mandate and validate qualifications and standards for cyber security professionals working in critical infrastructure environments.