Supplementary Submission
No 23a

INQUIRY INTO CYBERSECURITY

Organisation:	ISG Consulting Pty Limited
Date Received:	2 December 2020

27 November 2020

Chairman
NSW Upper House Cyber Security Review
Parliament House
Macquarie Street, Sydney, 2000

NSW Upper House Cyber Security Review

Following our interview as witnesses and consideration of the line of questioning of ourselves and other witnesses in the committee evidence taking processes, we submit the following observations by way of clarification.

The Committee was exploring the topic of national uniformity of approaches, which certainly is an important consideration. Some observations in relation to this are listed below:
ISO27001 and the other ISO27000 family of standards all have the advantage of having an agreed baseline of controls. These are all accepted globally as baselines for managing risks associated with Cyber Security. One of the real threats of moving away from a "standards based" approach to managing Cyber Security is that it is going to pose difficulties in the free exchange of information in the future with our trading partners. The adoption of a verifiable standards-based approach will mean overseas trading partners of Australian enterprises will have greater trust in our business and government organisations.

Why has the NSW Government slipped with regard to Cyber Security?
Risk Assessment is a business discipline that cascades through the business, feeding information from the "factory floor" up to the board level. It needs to be implemented within a suitable governance framework that ensures that the right information is making its way to the business leaders and forums responsible for setting policies, setting priorities, measuring the performance of business processes.

The concept of Cyber Security Agreements (CSAs) for line of business managers ensures that risk assessments are being made at an appropriate level of granularity at the business process level with respect to cyber security. These are based on RACI and are required to ensure that these security practices are pushed down and embedded into the business processes. The NSW Government with enterprises like Sydney Water Corporation, and Transport for NSW, pioneered these models within a certifiable framework. As far as we know the framework we have developed for the NSW Government is the only practical framework that has worked in NSW.

We don't support the decentralisation of responsibility for Cyber Security from a central agency in 2009 and believe that this has contributed to some of the problems being experienced currently. We welcome the recommendation to recentralise responsibility however believe that audit and review needs to be kept separate from policy and implementation.

The Essential Eight
While the adoption of the Essential Eight more broadly throughout Australian enterprises will assist with increasing resilience to cyber attack, we don't support its adoption as a separate initiative within the NSW Government. As a checklist it is fine, however a wholistic approach to addressing Cyber Security risks is preferable to the narrow focus of Essential Eight. We believe that the CIS Top 20 Controls, which addresses a broader range of priority controls, is a better approach for NSW Government agencies.

Role of the ISM
ISM was developed for Defence restricted facilities, and we believe that it's application outside of such facilities is of limited value.

Regards,

Mr John Frisken
Director – Professional Services

Mr Milton Baar
Director – Cyber Security