Dr. Oliver Guidetti • [redacted] • [redacted]

March 13, 2022

To the 2023 – 2030 Australian Cyber Security Strategy Expert Advisory Board,

My name is Dr. Oliver Guidetti, I am a post-doctoral research scientist working in cyber security. I hold bachelor's degrees in mathematics and psychology, with first class honours in the latter, and a PhD in Cyber-Security. More specifically, I specialise in Cyber-Psychology, the study of the human factors that drive the dominant majority of security problems in network defence.

This document outlines a series of responses to the 2023 – 2030 Australian Cyber Security Strategy Expert Advisory Board's Discussion Paper. These responses derive from my training and professional background in cyber security, and I feel they manifest a vital set of responses to the discussion paper. The humanity within the human user lays at the core of endemic problems we face in cyber today. Without giving voice to the human side of cyber security, this problem is likely to grow.

I hope this letter and the ideas it presents spark important discussions we need to have in Australia surrounding Cyber Security.

Kind regards

[redacted]

Dr. Oliver Alfred Guidetti
Email: [redacted]
Mobile: [redacted]
Address: [redacted]

Cyber Psychological Responses to the 2023 – 2030 Australian Cyber Security Strategy Discussion Paper

Three responses to the 2023-2030 Australian Cyber Security Strategy Discussion Paper have been outlined in this document and are structured according to the questions they specifically address.

Response One: Cyber WorkSafe

This first response refers to Questions 1, 2, 9, 13, 14, 15, 17 and 21 of the 2023-2030 Australian Cyber Security Strategy Discussion Paper.

Consider occupational health and safety (OHS) on building and construction sites. Back in the seventies, there was no such body as WorkSafe to police safe working standards around hazardous construction sites. When WorkSafe came along, industry resisted it at first but now it's as accepted a part of building and construction, as are ethics panels in research. Optus and Medibank demonstrate that the 2023-2030 Australian Cyber Security Strategy should include establishing a Cyber WorkSafe regulator, as big and sophisticated as WorkSafe is today. Cyber WorkSafe would be an organisation composed of cyber specialists whose entire role would be to police cyber security standards in businesses.

Different standards could be customised by industry and organisation size. For example, it should be harder to phish someone from a business like Optus than a smaller business like a café. The Cyber WorkSafe body should therefore function much like WorkSafe does today, by performing checks and tests of the cyber security state of businesses of all kinds and sizes. The Cyber WorkSafe regulator could fund their activities by fines they issue for violations of cyber security standards. For example, one such inspection that a Cyber WorkSafe inspector could perform is to see how many users in a business have a password that can be hacked in under a day. The password "oliver12345678910" can be cracked in 2.21 minutes according to https://www.passwordmonster.com/. In contrast the password "wVCCj!Q" would take two years to crack. The point this illustrates is that it would be far more egregious if a bank manager had a password like "oliver12345678910", than if a café owner did – however both correspond to different harms against our society. For instance, the bank manager gets attacked, thousands of people could lose their life savings, critical bank infrastructure could be in jeopardy, and more. In contrast, if the café owner gets attacked, then the harm is far simpler, smaller, and more contained. In both instances, the Cyber WorkSafe regulator would issue a fine based on the potential for harm done. That is, the bank manager should know better than the café owner, simply given the greater propensity for harm to be done if their password were cracked. In both instances, the regulator could issue a "crackable password fine" that would align with the degree of harm. The café owner could be fined say 1000 and the bank manager could be fined 10,000 and face more serious disciplinary measures for repeated violations.

Fines issued by Cyber WorkSafe could therefore be based on several factors.

1. Organisation size.
2. Organisation sophistication and criticality classification

3. Industry – for example, the same cyber security standard was violated by both the aforementioned bank manager and café owner example. However, the bank manager should receive a bigger fine because their violation maps to a far greater societal harm than the café owner.
4. Vulnerability sophistication. For example, a spear-phishing attack is more sophisticated than a generic phishing attack. Where a regulator finds a business is susceptible to unsophisticated attacks, this should be fined more heavily than the more sophisticated case.

The Cyber WorkSafe regulator should be able to fine both businesses and individuals within businesses alike. For instance, if the CTO of a major telecommunications provider uses "password" as a password to login to critical infrastructure, this is far more egregious a violation given the individuals position in the company. In such an instance, it may make sense to fine the company, for not adhering to the Cyber Security Watchdog's password standards, and the individual who should have known better given their position.

The Cyber WorkSafe regulator should also be responsible for benchmarking minimum cyber security standards that businesses must follow. For example, WorkSafe mandate that when a carpenter needs to work on the roof of a building, they must use a harness to mitigate the risk of falling.

That same standard does not apply to all organisations, so they have industry specific recommendations that apply to businesses of different sizes. The same could be performed by a cyber watch dog. When a business applies for its licence to operate, or its ABN, a part of that application could involve formally agreeing to remain up to date on standards and policies established by Cyber WorkSafe, just like builders have to do with WorkSafe.

Regarding Question 2f. It could be the prerogative of the Cyber WorkSafe regulator to decide on a case-by-case basis if ransoms and extortion demands made by cyber criminals are paid either by victims, insurers, or government. For example, if critical OT infrastructure at a port is infected by ransomware, this can map to significant costs to industry and port business partners, including influencing the stock valuation of business partners. Under such circumstances, the Cyber WorkSafe regulator could serve to answer the question: To pay or not to pay? This decision can be informed by working with the Ports cyber security team so it can establish how to triage the Ransome. Importantly, this example illustrates that government should not hold an "all-or-none" stance on ransoms and extortion demands, and instead establish the Cyber WorkSafe regulator to triage these crimes on a case-by-case basis.

Cyber Work Safe would be an ideal entity to operate, organise and run the reporting portal Question 13 refers to. Cyber WorkSafe could act on public reports of cybercrime, and where relevant, escalate incident responses up to higher professionals. For example, if the significant partner of a Bank Manager is successfully spear phished, then the Cyber WorkSafe operator that is called out to triage the incident can also check to see if the Bank Manager Partner was not also sent and fallen victim to the same phishing attack.

A final note of recommendation regarding the Cyber WorkSafe regulator. This should be a body large enough to perform checks of businesses of all sizes, scopes, and contexts. For example, the safety standards required to operate a major export port are context specific, likewise their OT security standards should also be context specific and monitored. A regulator of this size would also introduce thousands of new jobs in cyber, which could be serviced by the second response outlined in this document on K-12 Cyber Education.

Response Two: K-12 Cyber Education to Feed Cyber Industry

This second response refers to Questions 11, 15 and 17 of the 2023-2030 Australian Cyber Security Strategy Discussion Paper. There is a significant shortage of cyber security specialists in the Australian workforce, and our nation’s efforts to enhance our cyber security will only add to this demand. Migrant workers are one way of supplementing the cyber security workforce shortage, however this approach is neither sustainable nor entirely solves the problem in the long term. A sustainable solution to the cyber workforce shortage involves integrating cyber security training within the K-12 education system.

This response item calls on government to introduce Cyber Security as a new subject, distinct from Information Technology or Computer Science. The aim of this subject will be to offload cyber security training from the tertiary sector and deliver it to students across Years 11 and 12 of their education. The goal of this should be to begin to graduate school leavers who have a comparable level of cyber security knowledge as university students that have studied a bachelor’s degree in cyber security. The Bachelor’s degree in cyber security takes 3 years of full-time study.

We need to take those 2/3 years of that bachelor’s education, and distribute its content across the cyber security, information technology, and computer science curriculums taught to school students between years 11 and 12. The students who graduate with all three of these technological classes would then be able to complete a single years’ worth of training to complete their 3 years of training and become ready to enter the cyber security workforce. They may not fill more complex roles like a network security analyst, that role is typically reserved for students with both a bachelor’s and master’s degree. But they could perform in roles like that outlined in Response One of this document. Namely, they could become Cyber WorkSafe regulators. Operators with enough training in cyber security to specialise in checking businesses are meeting their cyber security obligations. This could be a career path with built in growth. Cyber Work Safe operators could begin auditing the cyber security of small businesses. Over time and with increasing workplace training, they could begin to work in the regulation of cyber security standards of increasingly larger and more complex businesses.

This would also enhance what can be accomplished in the university space. If students who graduate this program need only 1 year of training to reach parity with our cyber security undergraduates today, then the Bachelor of Cyber Security in the future could teach content currently reserved for master’s students. This one change to how we currently educate cyber security specialists means future school leavers are comparable to current undergraduates. Similarly, future cyber security undergraduates would be comparable to current students with a master’s degree.

Children are our nation’s future, which is why we need to implement this recommendation in response to Questions 11, 15 and 17, as it provides a ground up solution that could future proof our national cyber security posture well beyond 2023 and 2030. These are chances that need to be committed to today, so we can steadily implement them along with industry and university coordination over the next 7 years if we as a nation want to future proof cyber security in our society. All it would take is an acceptance that the subjects school subjects are currently being taught are simply not meeting the needs of our workforce, and that if left untended, this problem will metastasise in complexity and severity as time goes on. This approach produces a steady reliable stream of cyber security operators who will facilitate a culture wide upgrade in Australian cyber security.

Response Three: A Federal Whole of Government (WoG) Model of Cyber Governance

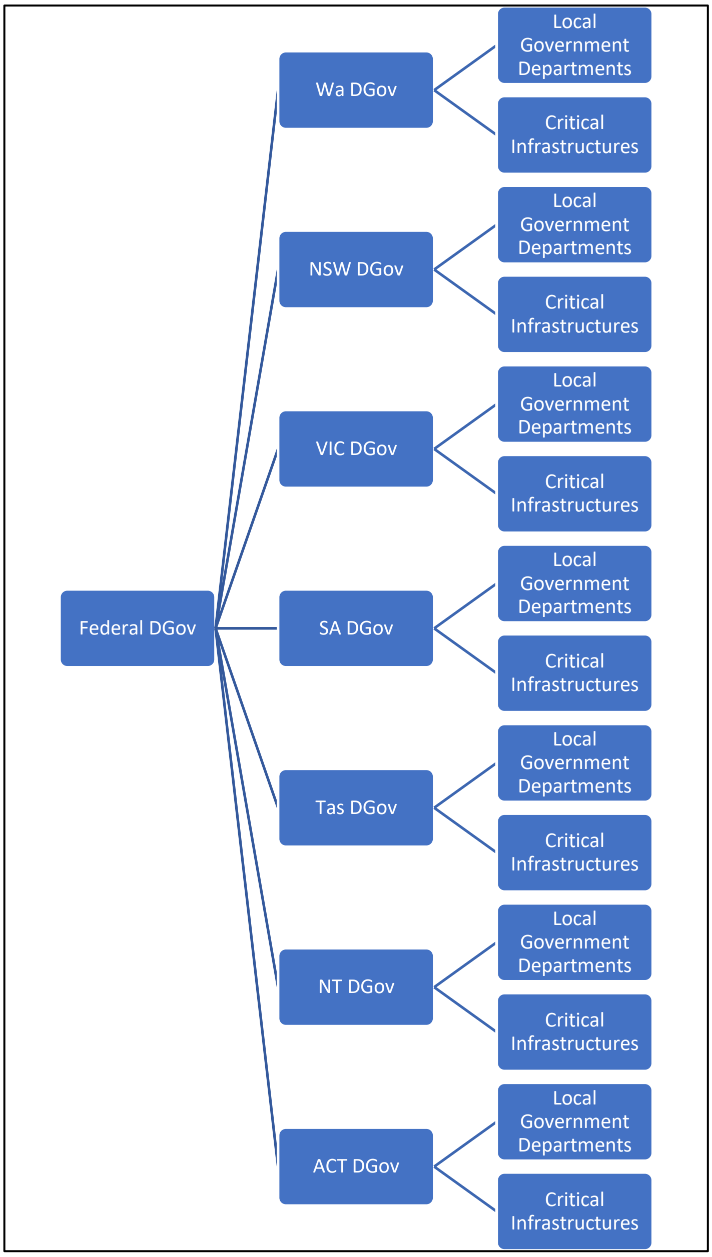
This section outlines a response to Questions 6, 7, 10, 19 and 20 of the 2023-2030 Australian Cyber Security Strategy Discussion Paper.

The Whole of Government (WoG) model of cyber security governance, pioneered by The Western Australian Department of the Premier and Cabinet’s Office of Digital Government (DGov) needs to be extended to a federal model. The DGov Cyber Security Operations Centre (CSOC) monitors and manages incident responses to cyber security issues in government bodies across the state. These bodies connect their security information into the DGov CSOC, which acts as a central node by which to respond to cyber incidents.

This model needs to be extended, so that every state has a comparable CSOC, all of which can then connect to a centralised federal SOC (Figure 1). This model would provide the federal government with a comprehensive perspective of the state of cyber security in the country, as well as top level insight and intelligence into national cyber-attacks. Security breaches in a WA government department might also occur elsewhere in another state. But without interconnecting each state’s DGov CSOC with a centralised Federal SOC, each state is left to deal with cyber-attacks on an individual basis. This is not only inefficient, but we also miss critical top-level intelligence, attacks of this magnitude will most likely reflect about nation state actions. With each state’s DGov operating in a siloed, disconnected way, the federal government cannot as easily triangulate national intelligence on cyber-attack coordination.

Figure 1

Whole Of Government Cyber Governance Model.



A federal WoG cyber security and government body could also be responsible for coordinating incident response measures that don't directly involve governing bodies. For example, this could include freezing trading of publicly listed companies that get attacked and identify threats in the cyber landscape that necessitate a legislative response. Moreover, such a governmental body would enhance Australia's capacity to detect and respond to nation state against the system as a whole. This should be a Whole of Government effort, and the ideal candidate to lead this endeavour would be the Coordinator for Cyber Security.

Response Four: Specific Commentary on Governments Position on Ransomware

The position of government with respect to payment or non-payment of ransoms by companies, should be one of caution. There will be circumstances where they must step in and show leadership. A component of the Federal Whole of Government (WoG) Model of Cyber Governance should act to deliver this leadership, a mechanism that ransomware situations and decide on a case-by-case basis if payment is appropriate. For instance, if a hospital is attacked, people’s lives may be in jeopardy, much more than just their personal information. Government should retain the right to decide when to pay and when not to pay a ransom. In the meantime, a research bounty should be established to give law enforcement tools that facilitate rapid responses to ransomware attacks and allow us to Hack the Hackers.