2023-2030 Australian Cyber Security Strategy

Andrew Ginter, VP Industrial Security
Courtney Schneider, Cyber Policy Research Mgr
Waterfall Security Solutions

Thank you for the opportunity to respond to the discussion paper regarding Australia's Cyber Security Strategy. Australia's stated goal of becoming the most cyber secure nation by 2030 is an ambitious one. The goal is analogous to France's stated goal of becoming a "cyber defense superpower." Both goals speak to ambitions to develop defensive rather than offensive capabilities.

Australia's goal is achievable, but will require a concerted effort on the part of:

- lawmakers,
- government funding for national implementation, enforcement, and research efforts,
- education institutions and
- the nation's most important government offices, businesses, and critical infrastructures.

Waterfall Security Solutions is one of the world's leaders in OT / critical infrastructure cyber defense. We are headquartered in Israel and have customers all over the world, including in Australia. We support Australia's defensive ambitions. We are taking this opportunity to respond to those questions in the discussion paper that we believe we are qualified to answer, based on our expertise, experience and customer relationships.

A high level comment before we begin – in our opinion, that Australia seeks to become a defensive superpower in cyberspace is entirely appropriate. China is a cyber offensive superpower. Given recent strained relations with China, Australian government agencies, critical infrastructures, businesses and private citizens must expect to be targets of the world's most sophisticated of nation-state and intelligence-agency attacks. This is in addition to being targets of ransomware criminal groups – groups that today are trailing nation states by less than half a decade in terms of the sophistication of their attack tools and techniques. In our opinion, Australia can become the world's leader in cyber defenses, or can suffer unacceptable consequences of cyber consequences – there is no third alternative.

The good news is that very strong cyber defenses are both possible and practical, in all three realms of classified government networks, business IT networks and operations / OT networks. By thoroughly committing to become a defensive superpower, Australia will both become an extremely difficult target to attack, and will develop domestic technology and expertise that can be exported to assist other nations and enterprises along the path to similar defensive capabilities.

Australia's need for strong cyber defenses is not unique. What stands to become unique is that almost no other country in the world is working towards this goal. By committing to this goal, Australia stands to become a leader in a space that in the years ahead will become very much in demand by all nations who use computers for government, business and industrial automation.

Please find our responses below. If you have questions about these responses, please feel free to contact us directly at:

Answers to specific questions follow.

(1) What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

To be effective, a cyber strategy must recognize a clear distinction between IT and OT systems, and between different kinds of systems within each sphere. Within the OT sphere, the strategy must recognize different levels of criticality for different kinds of industrial and critical infrastructure networks – networks whose worst-case consequences of compromise include unacceptable mass casualty events (eg: rail switching), environmental disasters (eg: offshore platforms), critical infrastructure service outages (eg: the power grid), and may also include acceptable business impacts (eg: small consumer goods factories) for which cyber insurance is easily available. Clearly distinguishing between unacceptable consequences and acceptable consequences of cyber sabotage is vital to designing effective and cost-effective cyber defenses.

Worst-case consequences of compromise should determine criticality, and criticality should determine the degree of cyber protections warranted for any individual asset, network or site. IT-grade protection is appropriate for business networks where worst-case consequences of compromise are acceptable business consequences – consequences for which business owners can purchase insurance for example. Much stronger protections must be deployed for military and government networks handling classified materials. Engineering-grade protections are needed for OT networks whose worst-case consequences of compromise are threats to public safety, critical industrial infrastructure service interruptions, or other unacceptable consequences.

Two recent developments in the United States are worth considering here. The US Transportation Security Administration (TSA) cybersecurity directives for pipeline operators and rail system operators (2021-02C and 1580/82-2022-01 respectively) were issued in response to the Colonial Pipeline attack. In those directives, the TSA requires operators to:

> *"Implement network segmentation policies and controls designed to prevent operational disruption to the Operational Technology system if the Information Technology system is compromised or vice versa."*

While this goal may seem obvious in hindsight, nothing like this was previously stated this clearly in a cybersecurity standard or regulation. Clearly defining specific goals such as this one is vital to effectively communicating the nation's need for cybersecurity to the many stakeholders involved in cybersecurity programs.

A second statement of principle from the recent US National Cybersecurity Strategy is worth considering for the Australian strategy as well:

> *"A single person's momentary lapse in judgment, use of an outdated password, or errant click on a suspicious link should not have national security consequences. Our collective cyber resilience cannot rely on the constant vigilance of our smallest organizations and individual citizens."*

Again, this statement of principle is profound. It means that important government agencies, critical infrastructures and other enterprises that are vital to the nation must deploy security systems so robust that they tolerate the most common human failures without risk to the organizations' mandates.

(2a) What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

Regulations should be seen as a last resort, when a nation's determined cooperation, education, funding and other initiatives have failed. This is because regulations frequently have unintended consequences. For example – the NERC CIP regulations in North America were so specific, and the non-compliance penalties so severe, that many power utilities put lawyers in charge of their security programs to ensure that the utility did not suffer massive compliance penalties. Worse, the CIP standards are so detailed that the paperwork involved in proving to an auditor that a utility has complied with the standards is very costly to produce and maintain. Poorly-designed regulations all over the world have resulted in large sums of money being spent on paperwork, sums that should have been spent more effectively on cybersecurity measures.

Waterfall recommends that Australia first pursue a very cooperative approach to dramatically improving cybersecurity. The government should first develop very strong expertise that is very specific to classified, IT and OT / engineering security and should make that expertise available to government agencies and private industry. Legislation may be necessary to establish and fund this mandate. Legislation may prove necessary as well to require agencies and businesses to cooperate with these experts.

A first deliverable for these experts should be strong guidance as to how classified, business and industrial networks should be defended. The most effective advice, however, is not yet another standard or document that parrots the NERC CIP, NIST, or IEC 62443 (OT) standards. All these standards describe the *minimum* that an entity or organization must do in order to comply. Australian guidance should be *aspirational* – describe the goal or end state that the nation needs of businesses. Describe a clear path to reach that state. Provide funding, education, and advice to reach that state. Provide guidance that describes the desired goal, not requirements for the minimum that every organization must do to become at least somewhat secure.

Specifically, this guidance should point out that critical industrial infrastructures / OT systems need engineering-grade protection from cyber threats for safe, reliable and efficient physical operations, in addition to more conventional IT-grade protections. The Australian government is encouraged to take inspiration from:

- ANSSI's *Cybersecurity for Industrial Control Systems* series of papers,
- Israel's *Reducing Cyber Risks for Industrial Control Systems*,
- *Secure Operations Technology*, ISBN 978-0-9952984-2-2,
- *Security PHA Review – for Consequence-Based Cybersecurity*, ISBN 978-1-64331-000-8, and
- The US DOE *National Cyber-Informed Engineering Strategy*,

All of these assets include descriptions of modern, powerful, engineering-grade protections for individual sites – protections that are in a real sense "unhackable." Engineering-grade protections are deterministic, empirically verifiable and mathematically modellable. The most consequential critical industrial infrastructures should all incorporate these techniques into their protections. Less consequential infrastructures should see this class of protection as aspirational – the Australian government should provide clear guidance to industry that OT networks generally should be protected in this way.

(2b) Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

The current *Security of Critical Infrastructure* act might make sense to lawyers, but is unfortunately impenetrable to cybersecurity professionals. Nobody wants lawyers put in charge of cybersecurity programs – that is a recipe for failure. Waterfall recommends that the act be re-written to become accessible to security professionals, so that these professionals can understand very clearly their obligations to their stakeholders and to the nation.

The act should also describe different obligations for different kinds of networks. On some networks, the goal is to protect information and prevent theft and mis-use of information. On OT networks, these goals must expand to include assuring safe, reliable and efficient operation of the physical operations that are essential to national critical industrial infrastructures, such as power and fuel delivery systems, water treatment systems, and transportation systems.

(2c) Should the obligations of company directors specifically address cyber security risks and consequences?

Yes, boards, and c-level directors should address and be responsible for cybersecurity risks and consequences, just as as they are responsible for other strategic enterprise risks. Any risk that poses a material threat to the mandate of the organization, or to the existence of the organization, should be dealt with directly by the board. This is not to say that boards should be involved in every decision about risk. Boards of course delegate. Boards should not be able to delegate dealing with strategic risks, however, and must ultimately, if indirectly, be responsible for all risks that a business undertakes.

Cyber risks, however, are singularly problematic for many businesses and boards. Cyber threats are evolving much more rapidly than any other threat that businesses and boards face today. The Australian government should not only remind boards of their responsibility, but should make resources available to boards, executives, and other stakeholders, providing guidance as to the nature of the threat and, again, aspirational guidance as to the kind of response the nation really would like to see from boards and enterprises, not only the minimum that enterprises must do to avoid litigation.

(2g) Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

If paying ransoms becomes illegal, then there must be a timely exception mechanism available for at least critical infrastructures in case of a cyber attack. When a crippled critical infrastructure risks becoming a national security issue, private industry must be able to call on the government on an emergency basis to find a solution to keep the infrastructure operational. Response from the government on these inquiries must be timely – failure of the most important critical infrastructures can cause irreparable harm to the nation within hours in some situations.

(4) What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

Waterfall recommends that Australian authorities partner with Israeli authorities to look at how Israel's critical infrastructure has become the most secure on the planet, and take inspiration from that progress.

(6) How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

In our experience, Australian organizations do not take strong direction from American, European, Commonwealth or international standards or best-practice guidance. Australian organizations tend to weigh input from local authorities and cooperative groups much more heavily than they weigh inputs from abroad.

The nation would therefore benefit from the Australian Government issuing its own aspirational and other guidance, whether that be inspired by documents, input or collaboration from overseas, or from local inputs. This guidance should be positioned within the context Australia's own economy, geography, foreign partners and adversaries, current average level of cyber defence across industries, local expertise, and local technology and service providers.

(10) What best practice models are available for automated threat-blocking at scale?

Attempting to identify attack sources and attacks in progress across the Internet may be worth while but is far from fool-proof. No such protection is engineering-grade. This class of

protection and investment by the Australian government may be cost-effective in the big picture of protecting an entire economy, but is no substitute for engineering-grade protection of physical operations, OT networks and critical industrial infrastructures.

(11) Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Designing protections for the most consequential OT networks demands a wide and deep skill set, encompassing elements of IP networking, operating systems, IT security, process engineering, safety engineering, automation engineering, network engineering, and other disciplines. It is generally not practical to acquire all of these skills in a single post-secondary program. On-the-job training, professional upgrading programs and other programs geared to IT professionals who are becoming familiar with engineering concepts and systems, as well as to engineers who are becoming familiar with computer, networking and cybersecurity concepts and systems, are all essential to Australia becoming a defensive superpower in the OT security space.

In addition, we advise that the government become involved with and incorporate into Australian training programs the security engineering body of knowledge that is currently being developed under the US DoE's *Cyber Informed Engineering Strategy* program. Engineering-grade protections eliminate entire classes of cyber threat and risk from the risk matrix, and do so essentially permanently. This emerging body of knowledge will very likely become very important in the years ahead.

(17) How should we approach future proofing for cyber security technologies?

Many of the OT-specific engineering-grade measures and resources described in our responses above are future-proof. These measures are in a real sense "unhackable." As unlikely as the concept may seem to IT professionals, engineering-grade protections can deliver reliable protection for OT networks from specific threats over periods of decades.

(20) How should government measure its impact in uplifting national cyber resilience?

An important and widely-neglected metric for critical industrial infrastructures is measuring the quantity, nature and quality of information that enters OT systems and networks. Namely:

- To assure safe, reliable, and efficient physical operations, industrial infrastructures must prevent cyber-sabotage.
- All cyber-sabotage attacks are information – the only way an industrial automation / OT system can change from an uncompromised state to a compromised state is if attack information somehow enters and affects the system.
- All information flows can include cyber-sabotage attack information.
- Therefore, a comprehensive inventory of all ways (both online and offline) that information can enter an industrial automation system is also a comprehensive inventory of attack vectors.

Secure industrial sites carry out such inventories and take measures to control or eliminate as many of these attack vectors as is practical. And when information must enter an industrial automation system:

- The most abstract information is more easily verifiable for safety than the least abstract, (eg: a short, ASCII XML file containing the instruction "produce 432 megawatts for the next 10 minutes" is safer than a 75 kilobyte file listing binary register values and setpoints for individual industrial automation equipment that – hopefully – has the same effect),
- Information that has been scanned for known malware is safer than information "fresh from the Internet," and
- Information that has been verified through detailed testing on a heavily-instrumented and heavily-monitored test bed is again safer than fresh-from-the-Internet or fresh-from-IT information.

Measuring and evaluating the quantity and nature of information that is currently entering critical industrial infrastructure networks is a powerful tool for understanding the exposure of such networks to cyber attacks.

Conclusion

Thank you again for the opportunity to contribute to your strategy deliberations. We hope the information and advice offered in the sections above proves useful to you.

A reminder: Waterfall has an Australian office. We welcome opportunities to cooperate with Australian authorities and other stakeholders in the country and in the region to improve the cyber defenses. For example, we welcome opportunities to participate in virtual or face-to-face meetings or workshops. We would be happy to meet with the government's technical and policy teams who are developing the national strategy to discuss these concepts at a next level of detail. There is no charge for such consultations – Waterfall routinely briefs government agencies free of charge. Please do call on us to explore whether and how we might contribute to supporting your mandate.

# # #