Dear Aus Cyber Strategy Team,

Forrester would like to respond to the 2023-2030 Australian Cyber Security Strategy. We do apologise for this submission being delayed and hope that you will still accept it for consideration. We understand how important the National Cyber Strategy Discussion paper is for the Australian Government's vision of making Australia the most cyber secure nation in the world. As this is a global issue, we have referenced our global research in compiling this response.

Forrester is one of the most influential research and advisory firms in the world, providing forward thinking research and advice to Government Leaders and their teams globally. Our unique insights and predictions are grounded in annual surveys of more than 700,000 consumers and business leaders worldwide, rigorous and objective methodoligies and the shared wisdom of our most innovative clients.

Forrester would like to respond to the following FOUR questions raised by the Strategy Discussion Paper:

- Question 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?
- Question 6: How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?
- Question 12: What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?
- Question 16: What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

We welcome further engagement, questions or discussions on any or all of the below. Please direct any queries to myself, on the signature details below.

Regards,

Jinan Budge she, her, hers
Vice President, Principal Analyst serving Security and Risk Professionals
mobile [redacted]
[redacted] Follow my latest research

I respectfully acknowledge the Traditional Custodians of the land on which I work. I also recognise the continuing connection to land, waters, and culture of Australia's First Nations Peoples and pay my respects to and their elders, past, present and future

Forrester Research, Inc.
Aurora Place, Level 14, 88 Phillip Street, Sydney NSW 2000 Australia
Forrester.com | Blogs | Podcasts | Twitter | LinkedIn | YouTube | Instagram

Question 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?

A plethora of ideas were contained in the Strategy Discussion Paper, as evidenced by the questions asked in the paper. There were two ideas which were notably absent, and Forrester would like to propose their inclusion in the final national strategy.

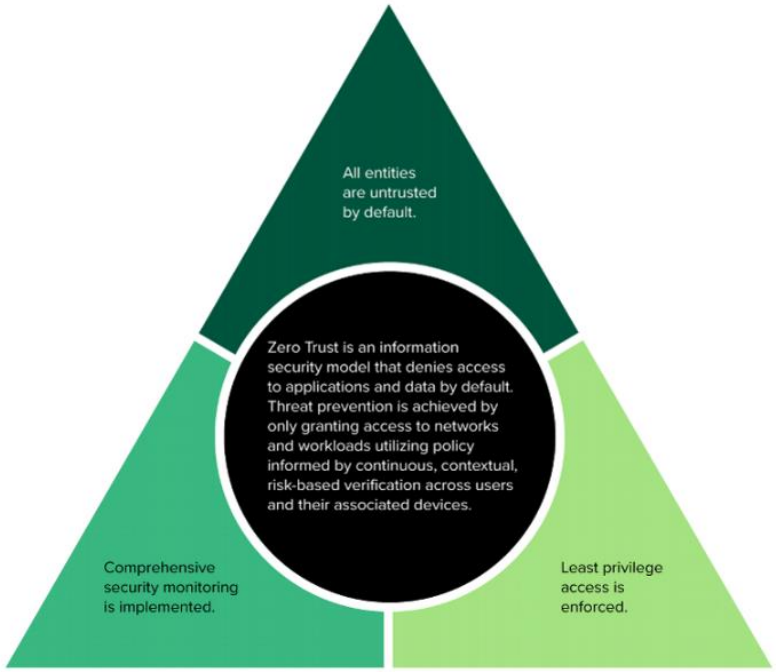
Idea 1: Adopting Zero Trust As The Modern Approach To Cyber Security

Forrester would like to see specific mention of Zero Trust ('ZT') in the Strategy, to be adopted as an overarching information security maturity model. Introduced in 2009 by Forrester, and going through an evolution in its scope and definition in the past few years, it is becoming a de-factor security model for a growing number of organizations in Australia. Since 2009, with the passage of time, a pandemic-created perfect storm of accelerated cloud adoption and remote work, the launch of Singapore Cybersecurity's Strategy, CISA, the release of President Biden's Executive Order, and NIST's release of its Zero Trust Architecture, "Zero Trust" is finally a familiar part of the nomenclature and vocabulary here in Australia, where there is a general acceptance of NIST cybersecurity frameworks. The formal definition is as follows:

> *Zero Trust is an information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their associated devices. Zero Trust advocates these three core principles: All entities are untrusted by default; least privilege access is enforced; and comprehensive security monitoring is implemented.*

Notice that the last sentence is the three original Zero Trust principles stated together. Here are the salient points of the definition in bullet form, and then in the figure following:

- Default deny
- Access by policy only
- For data, workloads, users, devices
- Least privilege access
- Security monitoring
- Risk-based verification



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Please see more information on ZT, and how it can be adopted, in ***our response to Question 6:*** *"How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities"*

Idea 2: Burnout in cyber security

Additionally, while the Strategy notes the importance of the cyber security workforce, Forrester would like to see issues relating to talent retention, specifically the issues of: a) burnout in cybersecurity; and b) attracting, retaining and advancing women in cybersecurity. We will be putting forward specific suggestions on both these issues in **our response to Question 12:** *"What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation? "*

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

Forrester would like to recommend that the Commonwealth Government adopts three practices to better demonstrate and deliver cyber security best practice, and serve as a model for other entities:

- Theme 1: Zero Trust ('ZT') to be adopted as an overarching information security maturity model for Commonwealth Government Departments.
- Theme 2: Adopting a human-centered approach to cyber security
- Theme 3: Move From traditional Security Awareness & Training To Adaptive Human Protection With Human Risk Management

Theme 1: Adopting Zero Trust

Introduced in 2009 by Forrester, and going through an evolution in its scope and definition in the past few years, it is becoming a de-factor security model for a number of organizations in Australia. Since 2009, with the passage of time, a pandemic-created perfect storm of accelerated cloud adoption and remote work, the launch of Singapore Cybersecurity's Strategy, the release of President Biden's Executive Order, and NIST's release of its Zero Trust Architecture, "Zero Trust" is finally a familiar part of the nomenclature and vocabulary here in Australia, where there is a general acceptance of NIST cybersecurity frameworks.

The Commonwealth can be proactive, lead the way in adoption, and get the many commercial, strategic, and leadership benefits that can come with being an early adopter of Zero Trust in the Asia Pacific region. To do so, Forrester recommends the following:

- **Gain familiarity with the modern definition of ZT.** Do this by reading and distributing the Forrester definition of modern Zero Trust. Publications by NIST, CISA, the White House, as well as the Singapore Government have become a driving force for ZT adoption in the region. While Forrester, which created ZT in 2009, refreshed its authoritative definition of modern Zero Trust in 2022, there is still confusion about the role of the many publications. Commonwealth Departments can overcome this confusion, and use the definitive definition of Zero Trust.

- **Assess ZT maturity of Commonwealth Departments.** Commonwealth departments can start by assessing the maturity of their Zero Trust environment. This ten-minute online resource asks only twenty targeted questions and gives you a score of beginner, intermediate, and advanced. Most organizations in Australia (and many overseas) will find themselves in the beginner state, which represents the conventional approach to cybersecurity. To achieve an intermediate level of Zero Trust maturity, orgs will have spent time and resources introducing Zero Trust network access, data flow visibility, and network microsegmentation around critical applications. The advanced level increases granularity of explicit policy, the depth of inspection controls and the breadth of the changes across your organization. For example, introducing host-level microsegmentation across both critical and important apps, and adding contextual verification and browser isolation into their zero trust network access.

- **Get some quick wins under your belt and demonstrate value that way.** Read Forrester's guidance to develop a roadmap to an intermediate state of Zero Trust. Plot each

Commonwealth Department's current business and security initiatives and setting the goal for your future state. Pursue quick wins such as the adoption of IAM technologies that solve critical problems and applying least-privilege principles if your organization is less mature. Or begin with more complex technical capabilities like microsegmentation if you work in a highly-regulated industry.

- **Challenge vendor claims and demand product rationalization.** With so much hype, vendors are trying to push their ZT products from all directions. In APAC, technology solutions such as IAM and Zero Trust Network Access (ZTNA) are often confused with ZT implementation. Security pros should demand that vendors show proof of their actual capabilities, rather than just marketing jargon. Vendors should be asked to produce their product roadmaps and support proof-of-concept (POC) activities. Forrester provides many publications such as The Forrester Tech Tide™: Zero Trust Threat Prevention, Q3 2020 and The Forrester Tech Tide™: Zero Trust Threat Detection And Response, Q2 2021 which help our clients to learn about solutions to support everything from micro segmentation to SOAR.

Theme 2: Adopting A Human-Centered Approach To Cyber Security

While the last decade has seen significant increased attention on cyber security, the proposed solutions, capabilities and skills have largely centered around technology. Many vendors use the defense in depth concept to justify whatever product they are selling. "You really need this, it is part of your defense in depth strategy." "This isn't designed to replace, but complement your existing security controls.". An ex-Forrester analyst, Rick Holland defined this concept as "Expense in Depth": the multilayered approach to ensuring minimal return on investment. In most cases we are getting diminishing returns on this additional investment. Add a global pandemic which elevated

We would like Commonwealth Departments, and more broadly organizations in Australia to recognize, or work towards the future of security being human-centered. While Forrester is still finalizing the definition of human-centered security, and how organizations can move towards that future, we offer the following as a draft:

Leading security leaders understand that security will always be about serving people — not only customers and citizens, but also employees, partners and society at large. They understand that the interaction of security technology with people and organizations is what matters. Therefore, these visionaries pursue a truly human-centered approach, shifting from forcing people into adopting security policies, processes and technology to enabling them to use it to their advantage. This research will seek to show security leaders how to help the business refocus on the people whose security experience will power their firm's brand promise, building trust in the brand, creative differentiation, and sustainable growth for decades to come.

Human-centered security organizations:

- Acknowledge the perspectives of the many people at the center of protecting information and systems

- Permanently prioritize people over technology, or at the very least, in parallel to tech. This includes designing user interfaces that enable employees to make good security choices, all the way to designing UX / UI of security tools well.
- Self-disrupt to focus on their own people and talent, including disrupting gender bias, developing and retaining talent, managing burnout and building trusted leadership.
- Engage and influence stakeholders all the way up, down and across their organizations
- Work relentlessly to shape security behavior, and instill a security culture, above and beyond perfunctory security awareness and training programs

Theme 3: Move From traditional Security Awareness & Training To Adaptive Human Protection With Human Risk Management

The regulations and standards driving security awareness and training (SA&T) programs are often outdated and confusing and have compelled organizations toward compliance as a strategy. This has caused organizations to measure the effectiveness of their SA&T programs with activity metrics like completion or phishing click rates, which provide no indication of behavior change or security posture improvement. Organizations must enable employees to perform their daily activities while protecting them from cyberthreats. The future state of SA&T is adaptive human protection. Adaptive human protection starts by instilling a security culture and adding capabilities so that people are hard-pressed to make the wrong decision. To get started on the journey to adaptive human protection, Commonwealth Departments must:

- **Quantify human risk on the basis of actual behaviors, not quiz scores.** Embrace the disruption introduced by human risk quantification vendors that take a data-driven approach to behavior change. Alternatively, some security teams quantify the risks of human actions via integrations with security tools to determine the risks posed by actual behaviors.

  Use the quantified results from these behaviors to allocate resources and initiate interventions when and where they are most needed. Intervention categories include policy based (e.g., blocking privileges of certain users) and training based (e.g., automatically adapting training according to the behaviors displayed).

  Track this over time to determine how human risk contributes to your overall cybersecurity posture. Choose the people, process, and technical mitigations necessary on the basis of how people behave; mitigations should include more than training.

- **Change and uplift the intent, scope, and nomenclature of your Security Awareness & Training (SA&T) program.** SA&T is a method, not an outcome. The desired outcome is to positively influence employee security behavior and instill a security culture. Unfortunately, SA&T tools fall far short of this goal, focusing instead on compliance.

  Modify the language you use to describe the program to reflect the goal instead of the method. This means changing your team and program names to show your intent, taking the lead from CISOs who have created digital user behavior teams, human risk management programs, or director roles for cyber influence and engagement.

  Making these small, yet foundational, changes sets the stage for how the program will be measured, the activities it's responsible for, and its overall objectives.

Question 12: What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

Complacency, lack of diversity, and a focus on technologies over people are all organizational threats. In an environment of competitive hiring and fast-evolving threats, Government must invest in professional development and growth for cybersecurity leaders and their staff to develop competence and create a positive team culture and environment built on empathy.

While finding and building competent security talent is essential to our nation's success and minimizing risk, it is not enough. Once we find or build that rare talent, we need to invest the time to lead and retain them. Ignoring retention practices will result in unhappy teams and cyber security professionals that hurts future hiring efforts, turnover that adds financial cost and disruption, disengaged employees that cost a fortune, toxicity in security teams that introduces risks to Australia, and a failure to retain women and other minorities that leads to a lack of diversity.

In response to those issues, Forrester suggests that the government supports the cybersecurity workforce through evangelizing, and funding programs which address the following talent related strategies:

1. Managing mental health and burnout of cybersecurity professionals
2. Attract, retain and advance women in Cybersecurity
3. Invest in security team culture
4. Retain key security talent with a clear path for advancement, developing an effective succession plan

Talent Strategy 1: Managing Mental Health & Burnout

Burnout is negatively impacting cybersecurity professionals' wellbeing and productivity. In 2022, we saw at a very practical level in Australia that weaknesses in our cyberdefenses can impact society at mass levels. The media and social media called out root causes such as misconfigured APIs, compromised credentials, bad development practices, and account takeovers — to a point that my mother, an immigrant doctor at the end of her medicine career (with minimal tech or security experience), was asking me to explain misconfigured APIs. But something that's seldom discussed in public forums when such breaches occur or, at least, not enough in my view — the people on the front line. They are the heart of cyberdefenses. They're doing all the defending. Yet how much do we think about them and their experiences at work? Are they supported? Are there enough of them? How do their jobs impact their mental health? What happens to customers, employees, and society if they are not taken care of?

- Forrester predicted that in 2023, a Global 500 firm will be exposed for burning out its cybersecurity employees.
- Soon-to-be-released research by a not-for-profit organization in Australia, Cybermindz, shows that cybersecurity workers scored significantly worse than the general population in one of the key burnout metrics of "professional efficacy"
    - Preliminary findings also show that they are suffering burnout at a rate higher than healthcare workers.

- A separate study of 1,027 members of security teams across the US and Europe shows that 66% of team members have significant levels of stress at work, 51% have been prescribed medication for their mental health, and 19% consume more than three drinks daily to deal with stress.
- Lesser-known impacts of burnout:
    - Talent retention - a recent study of cybersecurity in critical national infrastructure organizations showed that 57% of directors state stress and burnout as the top reason for leaving their position.
    - Productivity - 64% of security team members saying that stress has affected their productivity.
    - Reports of work-related deaths in Australia & China in 2022
- Our research on The People Leader's Guide To Burnout and Stop Burning Out Your Best People tells us to evaluate and address the inputs to staff burnout — for incident responders, for example, yes, ransomware is a heavy contributor to stress, but what also contributed to this stress is managing stakeholder expectations, lack of visibility and recognition, and receiving pushback on recommendations.
- Our leaders need to provide both physically *and* psychologically safe environments.
- We must ensure that cybersecurity teams have the tools, processes, and budgets to complete their jobs — there is a lot at stake, not just for them but for employees, customers, and society.
- And last but possibly most important, Government can work to normalize the conversation around mental health and burnout.

Talent Strategy 2: Attracting, Retaining And Advancing Women

Please see below from our contribution to Forbes, summarizing our research and recommendations for Best Practices: Recruiting, Retaining, And Advancing Women In Cybersecurity. Government can continue its work with AWSN on programs which address the systemic issues facing women in cybersecurity, and particularly considering the below recommendations.

For the majority of CISOs who are men (currently, 87% of CISOs at Fortune 500 companies are men and only 13% are women), there is an urgent need and enormous opportunity to become not just an ally but an outspoken champion for women in tech and cybersecurity, especially when so many people tell women to solve workplace challenges by simply "leaning in." While personal responsibility is important, there is only so far that your confidence can go in an industry ingrained with systemic sexism and bias. We need to do better and treat gender issues for what they really are: systemic business and social issues. For that to occur:

- **Make diversity, equity, and inclusion (DEI) a key performance indicator for your security team.** Too many detractors see these metrics as "unrealistic," when in fact organizations with diverse executive teams are 25% more likely to have above-average profitability. In a recent security services Forrester Wave™ evaluation, in which most vendors bragged about their DEI policies, the services firms that were the Leaders in the

Wave were the ones that actually put their money where their mouths are and tied DEI outcomes to their profits.

- **Mobilize male allies to influence change.** One of the most hard-hitting quotes we heard during our interviews was a male leader noting that "If one-quarter of all the men took a more active role in speaking out as an ally, doing just small things, we would make a significant difference." We learned that, far from being an accidental thing, true male allies go through a journey of personal and professional maturity, which starts with seeing and acknowledging that there's a problem, speaking out about even the slightest micro aggression, and continuous learning.

- **Avoid unpaid emotional labor.** Asking women to solve systemic sexism and bias workplace challenges can result in high levels of stress, compound feelings of difference, create additional workloads, and potentially lose time spent on career-related activities rather than accelerating cybersecurity practices. Some firms have started to acknowledge the cost of emotional labor — LinkedIn recently announced that it will pay its employee resource group leaders an additional $10,000 per year, and Twitter is following suit.

- **Model inclusive, supportive behavior.** Infosec Twitter spun up with news that DEF CON had banned a well-known Village leader for violating the code of conduct. Some wanted to know details and refused to believe the accusers without that information, but many prominent cybersecurity voices stepped in and defended the process and the accusers. As a leader, remember that your team will notice your response to external situations like these and decide whether they can trust you to help when they encounter bias and harassment.

- **Provide the tools and culture that encourage all employees to speak up.** Whistleblowers such as Susan Fowler and Alexandra Abrams are publicly calling out toxic culture, and they're naming names. But public disclosure is rarely the first step — in fact, 97% of employee whistleblowers choose to report internally first. Make sure your firm has the right technologies that enable anonymous internal reporting, a process to triage and investigate all internal claims, and a culture that not only supports but also encourages employees at any level to speak out against harassment and toxicity before it makes headlines.

Talent Strategy 3: Invest in security team culture

While remuneration is important in attracting talent, its impact on retaining that talent becomes limited over time. This means Government can contribute to how security teams in Australia are creating an environment that compels security staff to stay by moving beyond financial rewards, making work-life flexibility a priority, and cultivating a strong team culture.

This requires addressing the topic of toxicity within security teams. A toxic team culture causes the team to lose steam on critical cybersecurity projects. What does a toxic culture look like in practice? A team rife with infighting, unhappiness, and aggression between team members. At Forrester, We analyzed the top 10 causes of toxicity for security teams, the results of which are summarized in this blog. The research into this topic sadly revelated that many security professionals are experts on the subject.

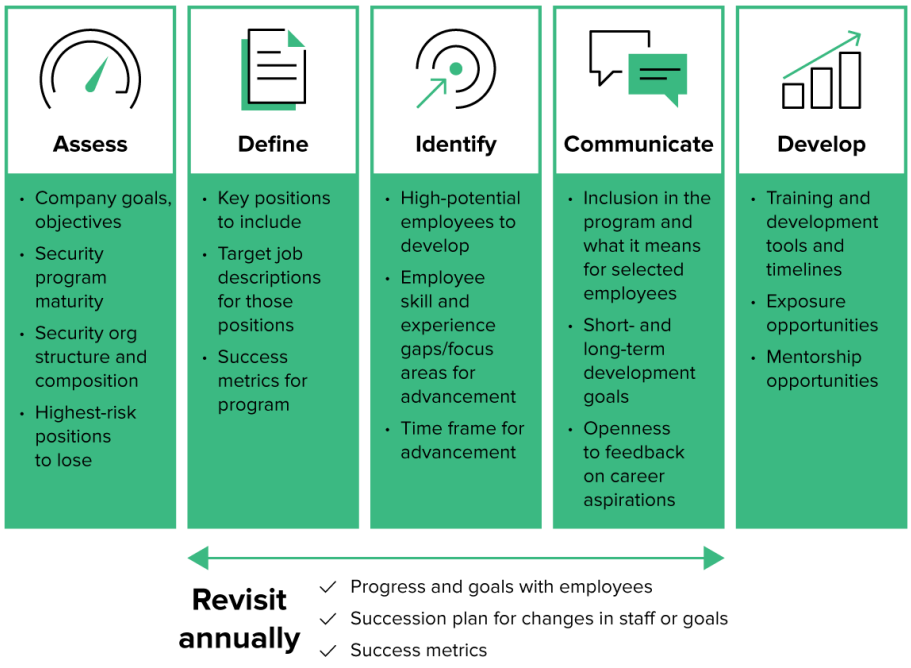
Government needs to fund programs creating strong, and psychologically safe teams. Such programs require the following:

- Investing in a portfolio of skills to prepare for the future of work. This includes technology and technical skills such as cloud security, risk management, privacy and ethics, communication and people leadership skills.
- Investing in prioritizing the emotional development of security professionals.
- Ensuring that organizations offer flexible work arrangements, and promote them.
- Prioritizing stakeholder relationships and engagement in hiring practices
- Invest in leadership training programs for security leadres

Talent Strategy 4: Effective Succession Planning

As we adjust to managing hybrid teams, and other business dynamics, we should also plan for the loss and replacement of key security talent. Attrition and the increasing length of time needed to find a replacement leaves security programs — and firms — vulnerable. Implementing a formal succession planning process for the security organization mitigates risk and increases employee satisfaction and retention. An effective security succession plan identifies future staffing needs and the people with potential, reduces the risk of lengthy vacancies for critical roles, and increases security's visibility. Government can work with enterprise to encourage building succession planning programs, taking the following steps:

Implementing a succession planning program for security



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Source: Succession Planning Is A Business Resilience Imperative, June 30th, 2022

Question 16: What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

Cybersecurity is one of the hottest areas worldwide for venture capital and private equity investment. There have never been so many cybersecurity startups globally. Unprecedented levels of investment have led cybersecurity startups to take new, innovative approaches to solving security problems.

Our research shows a great level of frustration as CISOs seek to avoid being used as guinea pigs for startups, fueled by lack of trust, time poverty, lack of organizational support and organization concern about financial viability of startups. In Australia specifically, we have seen years of praising and preferring solutions from the US and Israel, creating a culture where local startups are perceived to lack experience, depth and credibility. There has been a significant amount of work by AusCyber and others to counter this.

Government can further invest in training programs for CISOs to contribute to the innovation ecosystem, with special focus on:

- Actively supporting and mentoring security startups;
- Visiting startup booths in conferences to get an early view of emerging innovation;
- Playing fair and not copying IP from startups;
- Demonstrating value from investment in startups;
- Allocate funding and resources for using innovation in a security program;
- And utilizing startups' increased flexibility to meet security needs.