Google Australia Pty Ltd
Level 5, 48 Pirrama Road
Pyrmont, NSW 2009
Australia

google.com

24 April 2023

Department of Home Affairs
BY EMAIL: auscyberstrategy@homeaffairs.gov.au

Google welcomes the opportunity to provide feedback on the 2023-2030 Cyber Security Strategy discussion paper. Google supports the Australian Government's goal of being the most cyber secure country by 2030, and is committed to working with the Australian Government, States and Territories, and across industry as a trusted partner.

To make this vision a reality, we recommend that the 2023-2030 Cyber Security Strategy be designed as a roadmap that advances technology policies that put user protections first, promote innovation and technology modernisation, and explore new models of public-private partnership for collective defence.

Informing Google's global efforts to raise the bar on cyber security by improving our own security are the following principles:

- The best security solutions enhance openness and interoperability, rather than limiting them
- Transparency is essential to protecting users from online threats
- Digital technologies must be secure by default
- Security must become more intelligent
- Public-private collaboration is essential to raising the security bar for all.

These principles are relevant to consider in developing the 2023-2030 Cyber Security Strategy.

Google is committed to the security of the internet

Google has a long history in building secure infrastructure and helping to create and define cybersecurity best practices. Our approach to security – which emphasises a **focus on the fundamentals** of secure software development; an **open and transparent approach** to improving the ecosystem; and **pushing the frontiers of advanced security technologies** – have served us well and can serve as a useful roadmap for policymakers. We protect our users and enterprise customers by providing industry-leading security. We are committed to keeping users and customers, and Internet infrastructure more broadly, secure. We do

this in part by contributing to international security standards, sharing best practices, templates, developer tools, and providing other integrated solutions that make security stronger and easier to implement. And of course by offering secure services to our customers and users and implementing a shared fate approach to risk management rather than delineate where our responsibility ends.

Google's Approach to Security

Google takes a unique approach to security, which keeps billions of users safe online. Our approach is guided by a set of principles that we believe can help policymakers improve security. We believe people deserve products that are secure by default and systems that are built to withstand the growing onslaught from attackers. Safety should be fundamental: built-in, enabled out of the box, and not added on as an afterthought. That's why security is at the very core of every Google product. While others may tout their *security software*, our mission has always been to build *secure software* that can't be easily compromised by malicious actors. We do this by focusing on the fundamentals – prioritising secure software development practices, zero-trust architecture, and embedding security controls like multi-factor authentication which protect users by default. In other words, we take our responsibility as one of the world's largest tech providers seriously - increased collaboration between companies like Google and the public sector is vital to improving cybersecurity. Developing products that are secure by design is an important factor in the equation.

We believe **openness, interoperability, and transparency are fully compatible with strong security** - in fact we believe an open internet is a more secure internet. The internet was built on a foundation of multi-stakeholder governance, openness and interoperability, which created the conditions for one of the greatest expansions of opportunity and productivity in history. Disrupting this model would pose profound risks to businesses, institutions and ordinary users across the ecosystem — not least to their security. We are committed to driving up global security baselines through open standards and best practices. And we believe that technical standards which are guided by multi-stakeholder governance processes, open debate, and global security researcher engagement provide a far better, more inclusive path to trustworthiness. Google is committed to contributing to a vibrant open source ecosystem and as such, we are a key contributor to open source security projects, such as SLSA and regularly share our perspectives on open source (discussed in more detail below). We are also committed to being transparent about what we know about threats and vulnerabilities. Project Zero is a global leader in driving transparency around dangerous vulnerabilities, and our Threat Analysis Group alongside Mandiant (now a part of Google) drives global understanding of the threat picture (discussed further below).

We **develop advanced capabilities to help raise the security bar for all**. That's why in 2021 we pledged to invest $10 billion in global cybersecurity innovation and in partnerships with industry peers, governments, and civil society groups to solve previously intractable problems. We offer broad access to advanced security tools, such as zero trust, DDoS protection, and software supply chain security solutions, for users and organisations– tools that were previously out of reach for the vast majority of organisations. And we are **investing**

heavily to solve over-the-horizon security challenges, such as those posed by the evolution of artificial intelligence and post-quantum encryption. It is vital that government and industry partner to develop these advanced technologies to stay ahead of the threat.

Protecting Google's users, and customers

Security is the foundation of our organisational strategy. We've spent the last decade building infrastructure and products that are secure by design and implementing security at scale. By way of example:

- Every day Gmail blocks more than 100 million phishing attempts and 15 billion spam messages that never reach our users and customers
- Gmail blocks more than 99.9% of spam, phishing attempts, and malware from reaching users
- Google Play Protect scans over 100 billion apps for malware and other issues
- Every year we block billions of bad ads - on average 100 per second - through a combination of live reviewers and sophisticated software, and
- Safe Browsing on Chrome helps keep users secure from bad websites, automatically protecting more than 4 billion devices.

Making technology for everyone means protecting everyone who uses it. We're committed to building and sharing privacy and security technologies that protect our users and push the industry forward. We have a number of resources and information that we share with our users, including security tips to stay safer online.

As part of our enterprise services, Google Cloud's threat intelligence and cybersecurity teams are constantly on alert for potential threats to our customers, our systems, and the integrity of our platforms. Our approach is security that is built-in by default to our platforms through defence in depth layers and zero-trust principles to protect against the impact of malicious cyber activity, and eliminate entire classes of threats. In addition, we ensure the provenance of our software to minimise the risks of compromised supply chains.

Google also provides security protections and services to users and organisations around the world, including:

- **High-risk user protections**: Our Advanced Protection Program protects the accounts of high-risk users, including many journalists and activists. The program is free to enrol for any Google account user. We also provide free Security Checkup services to spot risky passwords and enrol our users in two-factor authentication automatically.
- **Cloud security visibility and controls**: Google Cloud offers a free version of our Security Command Centre to help customers strengthen their security posture by evaluating their security and data attack surface; providing asset inventory and discovery; identifying misconfigurations, vulnerabilities and threats; and helping mitigate and remediate risks.

- **Open Source security:** Google continues to be one of the largest maintainers, contributors, and users of open source and is deeply involved in funding research and helping make the open source software ecosystem more secure through efforts including the Open Source Security Foundation (OpenSSF), Open Source Vulnerabilities (OSV) database, and OSS-Fuzz.cu
- **Anti-fraud tools**: The free tier of reCAPTCHA helps organisations defend their websites against cyberattacks like credential stuffing, account takeovers and scraping.

Clarify and harmonise existing regulatory requirements

A key objective of any regulatory or compliance oversight should be to harmonise, streamline and avoid duplicating the regulatory frameworks applicable to the sector the subject of regulation. The development of the 2023-2030 Cyber Security Strategy provides the Government with the opportunity to consider existing requirements, and streamline (or enhance) frameworks to promote cyber security best practice and lift the security posture of all businesses and governments. Consideration should be given to harmonisation of domestic regulations and those in other countries where commercial providers might be conducting business; there are a growing number of cybersecurity regulatory and reporting requirements across the globe.

Recommendation 1:

- Ensure any new regulations are consistent to existing obligations, and that they support a robust national and international cybersecurity ecosystem
- Coordinate with international partners as to develop cybersecurity regulation, and use successful regulations as models for consideration in Australia.

Enable the adoption of open, interoperable, and transparent security technology

As noted above, Google believes openness and transparency are fully compatible with strong security. We are committed to driving up global security baselines through open standards and best practices. And we believe that technical standards which are guided by multi-stakeholder governance processes, open debate, and global security researcher engagement provide a far better, more inclusive path to trustworthiness.

Implementing strong zero-trust principles, promoting critical infrastructure resilience through cyber risk mitigation planning, and including cybersecurity requirements in procurement rules are crucial for advancing the security of the digital environment. In many cases, moving to the cloud is the most cost-effective and secure choice to protect networks and systems. In addition to economic advantages, since many security features are built in, cloud adoption can improve an organisation's baseline level of security, and enable custom configurations and advanced features to meet an organisation's specific needs. Embracing every security update the cloud provides to protect networks, systems, and data is like tapping into a global digital immune system, which continues to improve based on the evolving threat environment. Increased adoption and competition between cloud providers, including on security features, also drives security improvements in the

overall ecosystem. Particularly for small businesses, governments, and critical infrastructure, moving to the cloud holds significant advantages when compared to on-premises computing environments and the in-house security resources they require.

Often, cloud-based infrastructure like Google's can offer security that is more robust than on-premise alternatives. Well-managed cloud environments act as a "digital immune system" that intelligently uses up to date information about threats, vulnerabilities, and ongoing attacks to create a feedback loop providing optimised protection. These systems can be dynamically configured to improve the efficacy of protections and controls automatically, with continuous integration and deployment.

Open security requires that organisations focus on the fundamentals of software development and embed security at every stage of the product life cycle, from design through deployment. Users should be confident that the data they entrust to their devices, browsers, or cloud platforms remains safe with minimal manual configuration on their part. State-of-the-art security should be seamless, ubiquitous, and seemingly invisible. For example, Google embeds strong ransomware protections in its devices, operating systems, and platforms like Workspace. There has never been a reported successful ransomware attack against a ChromeOS device.[1]

Google has made commitments to build a safer open sourced community, including joining the Open Source Security Foundation, and created a new "Open Source Maintenance Crew" — a dedicated staff of Google engineers who work closely with upstream maintainers on improving the security of critical open source projects. We've also pioneered an open source vulnerability rewards program, to reward discoveries of vulnerabilities in Google's open source projects. And to further our commitments to help organisations strengthen their OSS software supply chain, we launched Assured Open Source Software service. Assured OSS enables enterprise and public sector users of open source software to easily incorporate the same OSS packages that Google uses into their own developer workflows. Each year over 10% of Googlers contribute to open source software projects. Our experience leads us to conclude that modern digital security actually can come through embracing openness. Open approaches ensure we can rapidly adopt the latest innovations and allow more people to solve security challenges. But to fully unlock the value of open source, we need stronger public-private partnerships and dynamic policy frameworks to shore up security for everyone.

Recommendation 2:

- Embrace security solutions that enhance openness and interoperability, rather than limiting them
- Foster an ecosystem that promotes open security principles
- Invest in digital transformation to enhance ecosystem-wide security and resilience
- Facilitate a framework for the adoption of OSS software supply chain integrity, like SLSA

[1] Enhancing Cybersecurity and Digital Resilience in Europe

- Ensure availability of government resourcing for open source software security
- Encourage stakeholders to account for open source software appropriately in their supply chain risk mitigation plans, development of clear/responsible vulnerability disclosure plans and processes.

Improving software supply chain defences

Since the cyber attack on SolarWinds, governments have made significant strides in bringing attention to software supply chain issues and accelerated efforts to gain better visibility into the software they procure. Industry has stepped up to support victims and provide technical expertise when attacks take place.

At Google, we believe that software supply chain security is one of the most critical national security risks facing governments worldwide and we continue to urge industry, government, and open source community stakeholders to come together to address it. Governments in particular have made important strides in recent months and we're committed to building on that momentum to drive stakeholders towards common goals.

We recently released a report on Google's perspectives on securing software supply chains as part of a new research series on emerging security trends and how to address them. In this report, we outline a series of measures we believe policymakers should consider to improve software supply chain resilience:

- Ensure appropriate prioritisation of cyber security
- Map the software supply chain
- Identify potential software supply chain risks
- Develop software supply chain risk mitigation plans
- Consider security requirements for software procurement
- Ensure coordinated vulnerability disclosure plans are in place
- Pursue industry partnerships.

The lessons we've learned from various security events call for a more holistic approach to strengthen defences against software supply chain attacks. This includes a common strategy across various stakeholders that centres on three core pillars: 1) adopt best practices and standards for cyber hygiene 2) build a more resilient software ecosystem and 3) make investments in the future.

Beyond supporting open security principles and improving software supply chain security more generally, Google is working with our customers to uplift security as they go through digital transformation journeys. For example, Google is pioneering the shared-fate model for risk management in conjunction with our customers. We believe that it's our responsibility to be active partners as our customers deploy securely on our platform, not delineators of where our responsibility ends.

We applaud the recent Security-by-Design Guidance from the Joint Cyber Defense Collaborative and international Partners including the Australian Signals Directorate on Principles and Approaches for Security by Design and Default. This is a step in the right direction, and encourage government to work with industry to ensure procurement is guided by security, and vulnerabilities are minimised.

Recommendation 3:
Develop a common strategy across government, industry, academia, and the open source community to better equip all stakeholders with the tools they need to address software supply chain risk.

Definition of data under the Security of Critical Infrastructure Act (SOCI Act)

The protection of customer data should be paramount for any organisation, and is paramount for Google as reflected in our data protection commitments to customers in our Cloud Data Processing Addendum. Protections for personal information currently exist in the *Privacy Act 1988* (Privacy Act), which was also recently amended to increase the penalties on corporations following high profile data breaches in 2022.

We note that the review of the Privacy Act continues, with submissions only recently closing on the many recommendations for amendments to the legislation. We consider it is appropriate to enable the Privacy Act review process to be completed before any consideration of further protections to customer data. In any event, amendments to the SOCI Act to expand the definition of 'critical assets' to include customer data would warrant detailed consideration, outside of the cyber security strategy. We believe any consideration of the definition sections of the SOCI Act should be undertaken when Home Affairs begins a statutory review of the SOCI Act in 2023.

Recommendation 4:
Government should conclude all phases of the Privacy Act review before amendments to the SOCI Act are considered.

Align with international standards to uplift security

We welcome the Australian Government's focus on cyber security policy and growing efforts by governments around the world to address cybersecurity challenges. Google works with many stakeholder groups to develop and pursue a safe, open, inclusive and global online environment. This includes work with other players in the industry and standard-setting bodies like the International Organization for Standardization (ISO), World Wide Web Consortium (W3C), and the Internet Engineering Task Force (IETF) as well as regional standards bodies.

Alignment with international standards ensures best practices are utilised, promotes interoperability, and avoids introducing unnecessary and burdensome complexity. Wherever possible, cyber security regulations and obligations should be aligned to international standards and best practices. This avoids conflicting standards and reduces

complexity for customers of cyber security services and for companies providing products or services to the Australian market. Importantly, it would also help Australian companies seeking to enter export markets minimise development costs.

New regulations and obligations introduced by the Government should be technology-neutral and risk-based, and aligned to international standards and best practices. Global security standards such as the ISO 27000 family of standards (and cloud-specific updates in ISO 27017 & 27018) create a robust and comprehensive security management framework.

Broad regulatory cooperation on cybersecurity will promote secure-by-default principles for everyone. This approach will strengthen Australia's cyber security posture, and allow it to be a leader in uplifting security in the region. These steps can be adopted by countries with varying levels of cyber maturity to employ advanced cyber initiatives like detailed threat sharing and close operational collaboration. Given the interdependent nature of the ecosystem, we are only as strong as our weakest link. That means raising cyber standards in the region will improve the overall resilience for Australia.

Recommendation 5:

- Participate in Standards Developing Organisations to help drive the shared understanding of current and future cybersecurity requirements
- Incentivise increased industry participation in standards development processes.

Choose technical and specific controls, like encryption and strong cryptographic controls over strict data localisation requirements

In recent years, the spread of data localisation laws has been perhaps the most visible sign of a growing trend toward digital sovereignty and tighter national control over technological infrastructure. A June 2022 analysis by the Organization for Economic Cooperation and Development (OECD), for instance, identified more than 90 data localisation measures in more than three dozen countries.

Proponents of data localisation argue such measures are necessary to prevent the theft or destruction of sensitive data by criminals or adversarial nations, to protect sensitive data from extraterritorial access by foreign governments, and to ensure continuity of operations in case cross-border data flows are disrupted. However, data localisation mandates may pose serious risks to digital resilience and security, while stifling the economic benefits of cross-border collaboration and innovation. Although data localisation may offer governments the perception of control over sensitive data, it involves a necessary trade-off against resilience to external threats and risks. This is why technologically-savvy countries are exploring creative ways to back up government data outside their territorial boundaries. For example, in response to Russian provocations in cyberspace, the Estonian government partnered with Luxembourg in 2015 to establish a "data embassy" to host sensitive records in a protected facility.

Data localisation requirements can also undermine security and resilience by preventing organisations from scaling resources to combat denial of service attacks or failing over their data to more secure locations when threatened by a natural disaster or armed conflict. For example, the Ukrainian government reversed previous policies requiring data localisation when the Russian invasion threatened its physical data infrastructure – instead seeking other mechanisms to advance resilience, including use of cloud capabilities for data storage.

Networks like Google's are global by nature, and imposing data localisation requirements could negatively impact resilience by reducing the availability of backups in disaster recovery scenarios. Furthermore, by particularising the provision of services from customer to customer and reducing the available workforce, these approaches are also likely to reduce the overall interoperability of services and portability of customer data, both of which help to ensure survivability and continuity of operations in exigent circumstances.

Availability, disaster recovery, and business continuity are an essential part of running a business or providing government services in today's digital economy. Unfortunately, earthquakes, hurricanes, floods, and other natural or human-made disasters are also an inevitable occurrence. Organisations will not survive if they do not have the ability to withstand and quickly recover from such events. Leveraging a globally distributed network like Google's infrastructure, which intelligently distributes data and applications through a geographically diverse network, enables businesses to confidently backup critical data and quickly recover and respond when disaster strikes. Laws, regulations or policies that require an organisation's data or applications to remain in one physical location dramatically increase the likelihood that a single catastrophic event will be insurmountable.

Rather than data localisation, setting foundational principles on strong encryption and customer control of encryption keys are superior means of protecting sensitive data than are requirements mandating where data is physically located. Google has pioneered Customer-managed encryption tools that give organisations unprecedented control over their data – including the ability to block cloud providers from decrypting their data for any reason – without sacrificing the universal availability and resilience that global infrastructure affords.

Recommendation 6:
Utilise technical controls to uplift the security of data, rather than imposing data localisation policies which may have significant negative impacts on the adoption of technology in the Australian economy and otherwise undermine data security.

Promote information sharing between governments and industry

We welcome growing efforts by governments around the world to address cybersecurity challenges. Meaningful improvement in cybersecurity will require the public and private sectors to work together in areas like sharing information on cyber threats; developing a

comprehensive, defensive security posture to protect against ransomware; and coordinating how they identify and invest in next-generation security tools.

The recent string of data breaches in Australia have underscored the need for closer threat intelligence sharing and joint incident response planning between governments and industry. To support this effort, Google regularly publishes and shares threat intelligence resources through channels such as the Threat Analysis Group's blog, Mandiant blogs and reports, quarterly Threat Horizons reports from Google Cloud, and regular Malware Trends reports from VirusTotal. Google's VirusTotal platform enables security researchers and practitioners in Australia and around the world to share information and expertise on the malware ecosystem, free of charge. Google would encourage other industry participants to equally engage in similar voluntary sharing of threat intel to uplift cyber knowledge which is critical to uplifting cyber resilience across the economy.

Information sharing alone is insufficient – there is more industry and government can do such as partnering on new open source and supply chain security frameworks, and building the cyber workforce. Google is committed to working with the Australian government and security industry to share cyber threat information, adopt technology to support cyber defence and facilitate security uplift across government and business.

Recommendation 7:
Engage industry and international partners to promote voluntary and reciprocal information sharing.

Evaluate using emerging technologies to contribute to national cybersecurity

Google believes that businesses and governments should modernise their approach to security operations to take advantage of automation to free up analysts for higher order tasks and artificial intelligence (AI) to respond to threats at machine speed. We bake in industry-leading security features (often invisible to users) and secure by default protections to keep our users safe. This includes technical controls, contractual protections, and third-party verifications or attestations.

One of the benefits of our experience using AI to solve real-world problems is that we have become better at helping secure new technologies as they become mainstream. At the same time, we're leveraging recent AI advances to provide unique, up-to-date, and actionable threat intelligence, improving visibility across attack surfaces and infrastructure.

We've recently shared our insights on how AI can improve digital security, and that to maximise the benefits of AI technologies and risks, Google takes a three-pronged approach:

1. Secure: helping organisations deploy AI systems themselves
2. Scale: leveraging the power of AI to achieve better security outcomes
3. Evolve: adopting a future-state mindset to stay ahead of threats.

We believe our approach reinforces a continuous cycle where frontline intelligence meets AI-powered cloud innovation, enabling businesses of all sizes to uplift their security posture through the adoption of cutting edge technology.

Recommendation 8:
Consider the use of emerging technologies to protect organisations, scale security and stay ahead of threats.

Harmonise reporting and uplift security practices across the economy

With the increased visibility of cyber attacks in Australia in the last year, we understand the Government's ongoing concerns around the need to report and remediate cyber security incidents and data breaches.

We note obligations for incident reporting exist in various regulations and policies, depending on the industry in which a business operates (e.g. CPS234 for financial services institutions, mandatory data breaches under the *Privacy Act 1988*) or exist following amendments made to the *Security of Critical Infrastructure Act 2018* (SOCI Act) in 2021 and 2022. While some obligations are sector-specific, generally they are not exclusive, meaning that a single incident may trigger multiple required federal reporting flows even before other obligations (such as international reporting obligations) are considered.

Given the challenges that organisations often face in managing reporting obligations while a cyber incident is ongoing, Google would encourage the Government to adopt a model of interagency harmonisation and designate a single entity responsible for receiving reports, disseminating incident information and channelling follow up with the covered entity. The Government recently announced the creation of a Cyber Security Coordination Centre, with further detail to come on the functions and the support the Centre will provide. In the creation of this Centre, the Government may wish to consider how to consolidate the reporting of incidents across multiple government agencies and to assign a single point of entry into government.

Recommendation 9:
Designate a single entity responsible for receiving reports and disseminating information during cyber incidents.

Post-incident review and uplift security across the economy

We recognise the importance of sharing best practice and learnings to uplift security across the ecosystem. We offer the following observations regarding the utilisation of post mortem reviews, and how similar practices have been adopted recently in the US.

Google has a strong 'blameless post mortem' culture, built over many years. The goal of these blameless post mortem processes is to document an incident or event to foster learning from it, both among the affected teams and beyond. The postmortem usually includes a timeline of what happened, the solutions implemented, the incident's impact, the

investigation into root causes, and changes or follow-ups to stop it from happening again. Our goal is to share post mortems to the widest possible audience that would benefit from the knowledge or lessons imparted. Google has stringent rules around access to any piece of information that might identify an end-user, and even internal documents like postmortems never include such information.

The US has recently established the Cyber Safety Review Board (CSRB) pursuant to President Biden's Executive Order (EO) 14028 on 'Improving the Nation's Cybersecurity'. The CSRB serves a deliberate function to review major cyber events and make concrete recommendations that would drive improvements within the private and public sectors, and is co-chaired by government and industry. The CSRB has adopted the 'blameless post mortem' approach, and has published reports on large scale cyber events. Adopting a joint public private initiative similar to the CSRB in Australia would facilitate learnings across government and industry, support uplift of security practices across the economy and to raise awareness with the community.

A core principle to the adoption of a blameless post mortem process in Australia should be to maintain proper confidentiality around the details of the incident, to the extent the incident is not already in the public domain (for example, anonymising the company the subject of the attack, but identifying the relevant industry/sector in which the company operates). Companies are more likely to communicate and engage about an incident to the extent there is protection from public shaming.

Instead, an anonymised, blameless post mortem process will likely have greater success in garnering cooperation and support from affected parties, and have a greater chance of uplifting security practices across the economy through government and industry partnership to create a culture of learning, collaboration and coordination in resolving future incidents. Further, any such process in Australia would benefit from adopting the CSRB model where industry co-develops any reporting intended for public consumption.

With the core focus of these post incident review exercises being to learn from past incidents and support the uplift of security practices across the economy, the Australian Cyber Security Centre would be well placed to engage with industry and government to conduct the blameless post mortems, and co-publishing with industry relevant learnings. In particular, we caution against mandating disclosure of information from cyber security consultants (as opposed to the organisation the subject of the incident) involved in breach investigations, so as not to disproportionately discourage Australian organisations from migrating to public cloud providers or seeking the assistance of cyber security experts in the event of a cyber incident, for fear of how the reliance on same may subsequently be used against the company the subject of the incident, thereby undermining cyber resilience in Australia and globally.

Recommendation 10:

The Government:

- consider consolidating all incident reporting into one central government body to receive reports, disseminate information and channel follow up with the company reporting the breach
- consult with industry to establish an initiative similar to the CSRB to conduct joint post mortem reviews to improve collective response efforts, improve security practices across the ecosystem and raise public awareness of incidents.

Building a cyber workforce

There is a global shortage of cybersecurity professionals, and the problem is only getting worse. Solving this problem requires investment to educate and support cybersecurity professionals, at the same time as you ensure that your existing workforce can be more effective. Both private and public entities have a role to play. Encouraging a healthy pool of cybersecurity professionals in your country will strengthen the ecosystem for all organisations.

Like any organisation, governments must find and recruit diverse, skilled professionals. Surveys of the private sector can often be informative in setting expectations for these positions, but many requirements like bachelors degrees, specific high-level certifications, and years of experience tend to block capable and diverse talent from applying. In particular, they tend to exclude outside-the-box talent like hackers, veterans, the diverse and underrepresented communities.

Once in place, these cybersecurity experts need to be retained. The longer a given employee remains with the organisation, the more specialised knowledge and skills they acquire, and the value of the entire workforce increases. Frequent surveys of employees and reevaluation of salary expectations can provide valuable insight into how best to retain your workforce. A strong mission connection will help make their roles fulfilling and impactful. And creating a culture of cybersecurity where professionals are encouraged to ask questions, challenge the status quo, and adapt to change will help make these jobs rewarding.

And while working to create and expand pathways into cybersecurity is critical, it is also important to think of the demand side of this equation. The Government should consider how to increase the productivity and effectiveness of the cybersecurity workforce already in place. Giving the existing workforce more effective tools can also be a force multiplier. Rather than asking the workforce to run on-prem infrastructure, leveraging providers who can provide integrated security by default in the cloud can help staff accomplish more.

Google is breaking down barriers to create pathways to cybersecurity careers for all, regardless of background, skills, experience, or the stage in their journey. We're eager to partner to create a safer tomorrow through our comprehensive approach to bridging the cybersecurity talent gap. We're working with universities to support cybersecurity research and improve curriculum development, run paid work-and-study apprenticeships that teach hands-on, real-world experience, and partner with community organisations to support diverse and non-traditional cybersecurity professionals. With our expertise, new career

pathways, and industry partnerships, we're uniting against cyber threats to make a difference together.

Recommendation 11:

- Increase steps to recruit diverse, skilled cybersecurity professionals
- Create service and entry level programs for cybersecurity professionals into national cybersecurity work.

Invest in cyber education

The public and private sectors are not the only stakeholders in the cybersecurity ecosystem. Almost everyone uses the internet and technology to do business, communicate, and learn. The Government has a core role in elevating security awareness and habits of the public, using public campaigns and partnership to empower their citizens. When creating new material is not feasible or not practical, providing the public with access to reliable educational resources can bridge the gap to higher level cybersecurity knowledge.

Education provides a longer-term pathway to addressing the previously discussed workforce shortage. Scholarships-for-service, partnerships with higher education institutions, and government funded educational programs can prepare and encourage the next generation of public servants. And most importantly, it is critical that not only cyber professionals learn the importance, or at least the basics, of cybersecurity: judges, members of parliament, lawyers, and teachers all need a minimum level of education in order to make cyber-aware decisions in their own areas of expertise.

Ensuring that children can learn how to be safe on the internet can be one of the most effective ways of fostering a long-term environment of security. Introductory curriculums, such as the Be Internet Awesome campaign by Google, can begin to foster skills and interest in cybersecurity as soon as possible. And government campaigns, like the Cyber Security Agency of Singapore's Better Cyber Safe Than Sorry campaign helps citizens adopt secure online tools and understand how to spot malware or phishing attacks.

Recommendation 12:

- Invest in cyber education through formal and informal avenues throughout a professional's career
- Continue to create education campaigns for the public, making sure that you're inclusive of people with all levels of digital and cybersecurity awareness
- Partner with the private sector to educate all Australians
- Educate non-cyber professionals like judges, members of parliament, lawyers, and teachers on the basics of cybersecurity relevant to their fields.

Designing a strategy for now, and for the future

With the dramatic rise of state-sponsored cyber attacks and malicious actors online, we are more focused than ever on protecting people, organisations and governments by sharing our expertise, empowering society to address ever-evolving cyber risks and continuously

working to advance cybersecurity products and practices to build a safer world for everyone.

We welcome the opportunity to discuss our experience and to engage with the Expert Advisory Panel and Home Affairs as it develops the 2023-2030 Cyber Security Strategy.