Cloudflare Submission to the Consultation on Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

Cloudflare is the leading connectivity cloud company on a mission to help build a better Internet. We empower organizations to make their employees, applications and networks faster and more secure everywhere, while reducing complexity and cost. We are trusted by millions of organizations – from the largest brands to entrepreneurs and small businesses to nonprofits, humanitarian groups, and governments across the globe.

We first established a footprint in Australia in 2012 when we launched our 15th data center in Sydney (our network has since grown to span over 335 cities in 125 countries/regions). We support a multitude of customers in Australia with our world-leading security products and services.

And as a strong supporter of Australia's *2023-2030 Australian Cyber Security Strategy*, we appreciate the opportunity to comment on the *Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy* (Horizon 2). We commend the Australian Government for its focus on this complex challenge: the urgent need to uplift the cyber resilience of the nation's most vulnerable entities, Non-for-Profits (NFPs). These groups provide critical services and support to the Australian economy and society, yet they are often the most targeted by cyber threats and the least resourced to defend themselves. We believe the focus on NFPs is therefore not just a matter of protecting individual entities, but a critical component of a robust, whole-of-nation defensive posture. This approach aligns directly with Cloudflare's mission and our long history of protecting those who need it the most.

This submission provides our perspective on questions 8 and 10 of the *Policy Discussion Paper*, specifically focusing on NFPs, drawing on our direct experience protecting millions of websites, including some of the most targeted NFP organisations in the world. We would appreciate the opportunity to further discuss our comments and questions.

Question 8: How can industry at all levels and government work together to drive the uptake of cyber security actions by SMEs and the NFP sector to enhance our national cyber resilience?

Collaboration between government, industry and critically – civil society – is the most scalable and impactful way to drive cyber uplift amongst NFPs. This partnership should be built on leveraging the respective strengths of each party: the government's ability to convene, provide resources, and set policy; industry's ability to innovate, execute, and deliver security solutions;

and civil societies' understanding of the threats facing NFPs, as well as the networks and trust that established civil society organizations have built amongst the communities.

Support Public-Private Partnerships

The most effective way for government and industry to collaborate is through partnership models that deliver training and information sharing, as well as driving greater awareness amongst NFPs of available services and resources. Cloudflare has extensive experience in various types of government and civil society partnerships globally.

Large-scale government initiatives have the ability to highlight critical security gaps and rapidly improve cyber security adoption and protection. For example, when the U.S. White House launched its National Cybersecurity Strategy in March 2023, then-Acting National Cyber Director Kemba Walden highlighted challenges faced by public school districts, stating "we expect school districts to go toe-to-toe with transnational criminal organizations largely by themselves. This isn't just unfair; it's ineffective." As part of the roll out of that strategy, Cloudflare developed and launched Project Cybersafe Schools – free email security and DNS filtering for eligible school districts – in collaboration with officials from the **Cybersecurity & Infrastructure Security Agency (CISA)**, the **Department of Education**, and the **White House.** One year after launching our program, nearly 120 qualifying school districts across 30 states have enrolled.

Governments can also work directly with NFPs help to create approved channels for the delivery of services to vulnerable communities that are regulated. For example, the U.S. Federal Election Commission (FEC) granted approval for a third-party non-profit organization to approve and coordinate donated cybersecurity services by certain private sector companies to US federal election campaigns. The agreement allows Cloudflare and other cybersecurity providers to donate such services in a nonpartisan way, without raising concerns under US federal election law. **As a result, Cloudflare now protects more than 60 US federal election campaigns and 20 political party domains through the program.** Protecting these sites has also allowed Cloudflare to collect data and threat intelligence regarding cyberattack trends against political campaigns, which is then able to report back to participants and the public.

Governments can also provide grants and other support to larger NFPs that work with industry to jointly provide services to smaller NFPs. For example, Cloudflare relies on 56 trusted civil society organizations around the world to help us identify and support groups who could benefit from Project Galileo, our program to provide free, robust cybersecurity protection to human rights defenders, journalists, and other at-risk nonprofit organizations. Our partnerships with these NFPs allow us to continually expand our reach to provide tools to communities that need protection the most. Many of those organizations, however, depend on government funding to support their cyber assistance efforts.

The government should also consider expanding support for NFPs that provide cyber security service and training directly to other NFPs. For example, the CyberPeace Institute provides cyber security assistance and data-driven insights on the threat landscape for NFPs. Through a

partnership with Cloudflare, the organization is also directly onboarding and managing email security services for other NFPs participating in CyberPeace's Cyber Peace Builders program. This approach not only streamlines cybersecurity adoption by participating organizations, but it also allows CyberPeace to serve as a central hub to aggregate real-time data on email threats through its online tracer.

Cloudflare has launched a partnership supporting vulnerable groups in Australia. General Practitioner (GP) clinics are the foundation of community health in Australia, holding vast amounts of sensitive patient data while often being under-resourced, making them prime targets for attacks that can halt patient care. To address this vulnerability, Cloudflare partnered with the **Critical Infrastructure-Information Sharing and Analysis Centre** (CI-ISAC) to create Project Secure. Through this program, Cloudflare will provide at-risk GP clinics with enterprise-level Zero Trust security solutions at no cost—specifically Cloudflare Gateway to block internet threats and Cloudflare Access to secure internal applications. Crucially, CI-ISAC will provide these clinics with free ongoing membership, giving them access to tailored, healthcare-specific cyber threat intelligence. We plan to expand this offering to a broader group of CI-ISAC members that need this foundational cyber support, but typically lack the resources and knowledge to do so. The challenge we have found with this program is generating awareness amongst the wider GP clinic communities that this program is available, something that government-industry collaboration as proposed would help to solve.

Curate a List of Vetted, Targeted, Easy-to-adopt Solutions

Rather than leaving small organisations to navigate a complex market, the government can lower the barrier to entry by curating and promoting a list of effective, easy-to-deploy, and low-cost solutions.

Governments have the ability to make these resources accessible and bring together multiple stakeholders to help promote best security practices. For example, in 2023, U.S. CISA – via the Joint Cyber Defense Collaborative (JCDC) – reached out to industry about an initiative focused on protecting vulnerable communities online, leading to the US CISA's "Free Cybersecurity Services and Tools" catalogue. This list, compiled by a trusted government agency, provides high-risk communities with a vetted selection of solutions, including Cloudflare's Zero Trust suite and a range of other industry cyber programs that are freely available for NFPs. This gives smaller organizations, like NFPs and SMBs, confidence that they are taking a meaningful step towards security without needing to become cyber experts.

Streamline Threat Intelligence Sharing

There are a very limited number of organizations monitoring and assessing cyber threats specific to civil society. In addition, most civil society organizations do not have the capacity to collect, share or ingest threat indicators, so this is an area that needs development and support from third-parties.

Industry has the earliest visibility of emerging threats. The government can help facilitate a streamlined, bi-directional threat intelligence sharing ecosystem that is targeted towards the needs of civil society. Industry can provide technical indicators, while the government can provide the platform for sanitised, actionable advice back to NFPs in a format they can understand and act upon.

Cloudflare provides a variety of threat information including global reporting on Internet traffic trends and shutdowns, DDoS and other cyberattack trends, and attacks on civil society organizations and elections.

Question 10: What are the unique challenges that NFP entities face for cyber security compared to the broader business sector and what interventions from government would have the most impact in the NFP sector?

Cloudflare has seen this firsthand when providing free cybersecurity services to vulnerable groups through programs like Project Galileo, and found that in aggregate, organizations protected under the project experience an average of **95 million attacks per day**. While cyber attacks are a problem across all industries in the digital age, civil society organizations are disproportionately targeted, many times due to their advocacy, and because attackers know that they typically operate with limited resources. In most cases, these organizations don't even know they have been attacked until it is too late.

Our experience protecting over **2,800 at-risk public interest organisations** globally through Project Galileo provides clear insights into these challenges.

Unique Challenges for NFPs

Relentless, Mission-Driven Targeting

Unlike businesses that are typically targeted for financial gain, NFPs are often attacked *because* of their mission. Human rights defenders, independent journalism outlets, and democracy advocates are frequently targeted by state-sponsored or politically motivated actors seeking to silence them. The scale of this threat is immense. Between May 2023 and March 2024, Cloudflare blocked **108.9 billion cyber threats** against organisations protected under Project Galileo—an average of **337 million threats per day**. The vast majority of these attacks are aimed at disruption – namely, looking to shut these sites down rather than steal sensitive data.

Cloudflare in July 2025 released a detailed analysis of threats that our Project Galileo NFP recipients faced between May 1, 2024, and April 30, 2025, broken down by sector and type of threats. Here are some examples of threats faced across the NFP ecosystem:

- **Journalism**: Independent media is a primary target. Overall, we protect 560 organizations that work in journalism and media around the world. Over the course of 2024, Cloudflare mitigated **97 billion requests**, an average of **290 million per day**.

- **Social Welfare**: Cloudflare identified over 800 social welfare organizations around the world that are protected under Project Galileo. These organizations support communities by delivering essential services such as food, housing, healthcare, and education. A study conducted in 2023 by the CyberPeace Institute found that 41% of these NFPs have been victims of a cyberattack in the past few years. Over the course of 2024, Cloudflare mitigated **1.5 billion requests**, an average of **4.47 million requests per day**, against social welfare organizations protected under Project Galileo
- **Environment**: Environmental organizations, including climate advocacy groups, are frequently targeted by cyberattacks. Under Project Galileo, we provide services to a range of groups that work in raising awareness on climate change, conducting scientific research, and providing the public with vital information during environmental crises. These groups often experience sudden surges in traffic and unexpected attacks during environmental disasters. Cloudflare surveyed 159 environmental groups and disaster relief domains protected under Project Galileo. Over the course of the last year, Cloudflare mitigated more than **1 billion requests**, an average of **3.7 million per day** against organizations working in environmental issues and disaster relief.

Finally, we have witnessed first hand the significant threats faced by school districts in the US**.** During the first year of Project Cybersafe Schools our cloud email security solution identified and blocked more than **2 million malicious emails and 2.2 million spam emails** targeting more than **40 enrolled school districts**. The consequences of these attacks can be severe: Recovery time can extend from two all the way up to nine months – almost an entire school year.

Increasing Volume and Sophistication of Attacks

Cloudflare has observed that the nature of attacks against civil society continues to evolve and break records. Our DDoS threat reports focused on civil society look at two key attack mitigations: DDoS mitigations and Web Application Firewall mitigations. When we looked at attacks towards independent media sites across Europe, for example, we saw an increase in attacks year-on-year. For reference, in our dashboard from the 2023-2024 reporting period, daily spikes never crossed the threshold of 4 billion requests. For the 2024-2025 reporting period, we have a multiple-day entry which surpasses that threshold by nearly 5 times. According to our data, DDoS traffic makes up 92.88% of mitigated traffic towards media organizations, with less than 6% of traffic identified as being blocked by the web application firewall. This clearly shows more DDoS attacks compared to WAF-blocked traffic, which attempts to exploit web vulnerabilities.

Severe Resource Disadvantage

Our experience is that NFPs operate with extremely limited budgets and rarely have dedicated IT or security staff. They cannot afford enterprise-grade security tools or the expertise required to manage them.

The CyberPeace Institute study referenced above, for example, found that 56% of social welfare organizations do not have a budget allocated for cybersecurity needs, while 70% do not believe they have the knowledge, skills, and resilience necessary to respond effectively to a cyberattack.

Reliance on Volunteers

We can see that NFPs often rely on a transient and non-technical volunteer workforce, increasing their vulnerability to social engineering and phishing attacks.

Most Impactful Government Interventions

Support NFPs that provide cybersecurity training, services, and other support to the NFP community

The single most impactful intervention would be for the government to fund grant programs that support civil society or NFPs specializing in cybersecurity services. One of the most important factors for NFPs to make use of cybersecurity services, including those available for free like Project Galileo, is accessing them with the assistance of a trusted partner. Organizations like the CyberPeace Institute, AccessNow's Digital Security Helpline, and many others, have earned the trust of organizations in their communities. Ensuring those services have the funding necessary to operate is essential to improving national cyber resilience.

Provide a Platform for Industry and NFP Collaboration

Our observation is that governments have the power, visibility, and resources to bring multiple parties together. The government can support multistakeholder convenings, including those led by NFPs, to bring together NFPs and civil society organizations for better training, information sharing, and collaboration.

Develop NFP-Specific Threat Intelligence and Guidance

As mentioned above, the government should work with industry and NFP peak bodies to develop and disseminate threat intelligence and guidance tailored to the unique risks faced by the sector.

Conclusion

Cloudflare stands ready to partner with the Australian government to discuss and help action the recommendations outlined in this submission. By focusing on simplicity, fostering deep public-private collaboration, and directly addressing the unique vulnerabilities of the NFP sector, we can collectively achieve the goals of the *2023-2030 Australian Cyber Security Strategy* and build a more secure and resilient digital future for all Australians.