goldilock

Submission for Horizon 2 Consultation
Goldilock Secure Pty Ltd

Executive Summary

Goldilock Secure welcomes the opportunity to contribute to the development of Horizon 2 of the 2023–2030 Australian Cyber Security Strategy. Horizon 2 aims to scale cyber maturity across the economy, establish consistent standards, empower businesses and citizens, and enhance the cyber workforce and ecosystem. Our submission addresses key themes identified during the consultation process, including the need for zero-trust architectures, enhanced sharing of threat intelligence, stricter controls for IoT and edge devices, and engineering-grade protections for operational technology. It also highlights that regulation should not only address post-incident response, but place greater emphasis on proactive, hardware-based measures to protect critical infrastructure.

Goldilock's principle of "Disconnect to Protect – on demand" reflects the view that network connections should exist only when required for legitimate purposes. FireBreak enables organisations to keep systems physically disconnected by default, with connections established only when operational needs arise. This approach applies across contexts, from enterprise data centres to remote water pumps, solar farms, and other operational sites, where systems can remain offline most of the time, connect briefly to transmit telemetry or carry out maintenance, and then return to a protected, disconnected state. The ability to manage disconnection and reconnection on demand is as crucial as emergency isolation during a cyber incident.

Our proposal centres on FireBreak, a hardware-enforced Physical Connection Controller that delivers real-time physical segmentation and controlled reconnection for both IT and OT environments. FireBreak complements zero-trust and attack surface management frameworks by providing a physical layer of defence, cutting connectivity in line with policy irrespective of software state. Embedding this capability into national cybersecurity measures would close current gaps in regulation, enhance resilience for critical infrastructure, and position Australia to lead in the application of hardware-enforced security.

Outlook for Horizon 2

Australia's cyber strategy must anticipate the technologies and attack methods that will define the next phase of the threat landscape. Developments such as AI-driven malware, IT/OT convergence, vulnerabilities in edge devices, and advances in quantum computing will continue to challenge traditional defences. At the same time, the growing exploitation of firewalls and other perimeter tools demonstrates the limits of software-only approaches. To remain resilient, Horizon 2 should embed physical isolation as a complementary safeguard to existing frameworks, while also addressing standardisation, incident response expectations, sovereign capability, and stronger public–private collaboration.

AI-driven attacks and autonomous malware

Attackers are utilising generative AI to craft targeted phishing emails, automate exploits, and compromise systems on a large scale. The frequency of AI-driven incidents is rising rapidly, and current software-based defences cannot guarantee containment. Physical isolation provides a last-line of defence and ensures that compromised segments cannot communicate with the rest of the network.

IT/OT convergence and increased attack surfaces

Critical infrastructure and industrial environments are increasingly integrating IT systems with operational technology (OT) for enhanced efficiency and remote management. This convergence exposes legacy equipment to sophisticated attacks. A hardware-enforced segmentation layer is crucial for preventing lateral movement and maintaining safety.

Edge devices and consumer energy resources

Edge devices deployed in critical national infrastructure, such as grid-connected inverters, substation controllers, distributed energy resources, and industrial gateways, are increasingly targeted by malicious actors. Compromising these devices can provide entry points into operational networks or be leveraged to disrupt wider systems. As standards for securing edge infrastructure evolve, FireBreak provides a practical safeguard by enabling these devices to be physically disconnected when not in use, thereby reducing their exposure and limiting their potential as attack vectors.

Data-driven AI and quantum computing

Large-scale data sets and future quantum capabilities will put existing encryption and privacy mechanisms to the test. Controlled, auditable connectivity windows between data repositories and AI training environments are necessary to prevent accidental data leakage or model tampering.

Growing exploitation of firewall vulnerabilities

Over the past 18 months, there has been a surge in critical vulnerabilities and zero-day exploits targeting major firewall vendors. As attackers bypass perimeter defences, the controls that organisations once relied on are fast becoming their weakest link. This trend underscores the need for a hardware-enforced fallback. FireBreak functions as the firewall's last line of defence by physically severing connections when software-based protections are compromised.

In addition to these trends, industry feedback highlights the need for standardised device security frameworks to address the growing risks of connected technologies. Approaches such as Manufacturer Usage Description (MUD) profiles, mandatory labelling for IoT devices, and zero-trust policies that automatically quarantine non-compliant devices demonstrate how consistent standards can reduce systemic vulnerabilities. These developments underscore the importance of incorporating hardware controls such as FireBreak, which can provide enforced segmentation and isolation to complement software-defined policies and strengthen overall resilience.

Strategic Factors For Government Consideration

Mandating physical isolation where appropriate

Logical segmentation alone is insufficient; physical disconnection ensures complete separation and eliminates the risk of remote compromise. The SOCI Act currently refers to segmentation but does not mandate physical isolation, creating a regulatory gap.

Rethinking incident-response timelines

International frameworks (e.g., EU NIS-2) require rapid reporting and containment. FireBreak facilitates instant isolation, enabling organisations to meet 24-hour reporting obligations and limit spread.

Supporting sovereign hardware capability

Goldilock manufactures in the UK (NATO-sourced components) and the U.S. (compliant with strict government supply chain standards), with no Chinese components. As an Australian sovereign company, we are prepared to establish local manufacturing and R&D to meet national security and supply chain requirements.

Fostering collaborative threat intelligence and reporting

Industry submissions consistently stress that threat intelligence sharing must move beyond transactional indicator exchange toward genuine public–private partnerships. A stronger national framework should provide central coordination through the Australian Cyber Security Centre (ACSC), supported by single reporting pathways and the expansion of Joint Cyber Security Centres (JCSCs) as hubs for collaboration. The strategy should also enable hardware devices such as FireBreak to contribute anonymised connection and disconnection events to sector-specific sharing platforms. This would enhance situational awareness across critical infrastructure sectors, strengthen national coordination, and do so without compromising privacy.

Collaboration and Evaluation

The effectiveness of Horizon 2 will depend on close coordination between federal, state, and territory governments, together with industry and the research sector. Consistent policies, shared standards, and a unified approach to capability development are essential for building resilience across critical infrastructure. At the same time, evaluation frameworks must be embedded from the outset to measure adoption, track outcomes, and provide government and industry with the evidence needed to refine policy over time.

Driving Adoption Through Pilot and Policy

Goldilock technology has already been tested and deployed in global critical infrastructure, enabling energy, water, and transport providers to isolate environments from cyberattacks in real time, physically. For Australia, adoption should be driven jointly by industry and the federal government, through pilot programs across key sectors (health, energy, transport) and supporting policy. Outcomes can inform national standards, funding models, and the broader integration of physical isolation into Australia's cybersecurity framework.

Embedding Layer 1 Physical Isolation into Training

Australia's cyber frameworks and the SOCI Act currently overlook OSI Layer 1, despite it underpinning network resilience and serving as a powerful defensive tool. For too long, this layer has been treated only as background infrastructure, and a significant re-education effort is needed to recognise its value. Embedding hardware-enforced disconnection at Layer 1 into policy would establish a new baseline for security practices, ensuring that TAFE and university programs train future practitioners in physical isolation as a core element of sovereign, hardware-based security.

Positioning Australia at the Forefront of Cybersecurity

Emerging technologies such as FireBreak are gaining traction across the U.S., EU, and UK. By moving early, Australia has the opportunity to lead rather than follow in adopting hardware-enforced isolation as part of its cyber defence posture. This aligns with international trends, where partners emphasise Zero Trust, attack surface management, and hardware security standards (e.g. NIST, CISA, EU frameworks). A cross-government taskforce could monitor these developments and ensure that Australia's standards for physical isolation remain interoperable, competitive, and globally recognised, supporting the national ambition to be a leader in cybersecurity.

Evaluation Framework (Appendix A Q3–Q4)

To measure progress under Horizon 2, outcomes should be defined and tracked through clear metrics. Suggested measures include;

Adoption rates
Number of critical infrastructure assets implementing physical segmentation, with baseline figures compared against post-initiative uptake across sectors.

Mean Time to Isolate (MTTI)
The time between detection and physical isolation during incidents. Hardware-enforced controls can reduce MTTI from hours to seconds, limiting damage and disruption.

Incident recurrence rates
Frequency of lateral movement after incidents in environments with and without physical isolation.

Compliance indicators
Proportion of organisations meeting SOCI Act obligations and international reporting requirements.

To support transparency, this framework could be complemented by public–private dashboards displaying aggregated adoption and compliance data, as well as the number of quarantined connections. Metrics could be collected by integrating device-level activity data with the National Cyber Intel Partnership's threat-sharing platform. Regular independent audits would validate reporting, ensure accuracy, and provide evidence for policy decisions.

Shield-by-Shield Responses

The Horizon 2 consultation has been structured around six strategic shields; each aimed at strengthening Australia's cyber resilience and positioning the nation as a leader in the region. The following responses outline how hardware-enforced physical isolation, through technologies such as FireBreak, can support these shields. They demonstrate how practical, enforceable controls can help protect critical infrastructure, empower small and medium-sized enterprises, strengthen sovereign capability, and build trust with international partners. Each shield response is aligned to consultation questions and grounded in measures that can be implemented across government, industry, and the community.

Shield 1 – Strong businesses and citizens

FireBreak supports Shield 1 outcomes by providing a practical and accessible form of physical segmentation that can be deployed by small and medium-sized enterprises (SMEs) and not-for-profit organisations (NFPs).

Awareness and Adoption (Q5–Q10)
Cyber awareness programs should include training on hardware-enforced isolation as part of standard cyber hygiene practices. A "Physical Segmentation Starter Kit" could be developed in partnership with the Cyber Wardens program, offering subsidised FireBreak units to SMEs and NFPs alongside guidance on installation and use. This would demonstrate that advanced protective measures are not limited to large enterprises but can be straightforwardly adopted by smaller organisations.

Insurance and Ransomware Risk (Q11–Q13)
Insurers often recognise discounts when strong risk mitigation controls are in place. FireBreak's ability to limit the spread of ransomware and protect backup environments could be acknowledged within cyber insurance frameworks. Government could work with insurers to formally recognise hardware isolation as a measurable security control, encouraging uptake while reducing overall exposure to ransomware-related losses.

Capacity Building for SMEs and NFPs
Industry submissions emphasise that smaller organisations lack the resources to implement complex security measures. To address this, a government-funded "IoT and OT Security Assistance Scheme" could be established. Accredited partners would help SMEs deploy FireBreak units, configure device security policies (e.g. MUD policies), and connect with threat intelligence platforms. This approach aligns with recommendations from IoT Alliance Australia for certified IoT devices and consumer awareness programs, while ensuring that smaller organisations are not left behind in the adoption of stronger security practices.

Shield 2 – Safe Technology

FireBreak provides a hardware-based control that directly supports several Shield 2 focus areas. By embedding physical isolation into Horizon 2, Australia can strengthen resilience, reduce systemic risk, and reinforce sovereign capability.

Resilience of Edge Devices and Operational Technology

The discussion paper highlights the increasing targeting of routers, firewalls, VPNs, and OT equipment. FireBreak enhances resilience by allowing these devices to be disconnected when not in use or immediately isolated in the event of a threat. This ensures that essential systems cannot be exploited through persistent connectivity.

Systemic Risk in Energy Infrastructure

Large-scale energy assets, such as solar farms, wind farms, and hydroelectric facilities, form part of Australia's critical energy system and are central to the transition to renewable energy sources. As these sites are increasingly integrated into the grid, they present systemic risks if compromised. FireBreak provides a way to isolate these assets during maintenance or when anomalies are detected, reducing the likelihood of cascading failures across the energy network. Embedding physical isolation into the protection of these assets would directly support the Australian Energy Market Operator (AEMO) and regulators responsible for safeguarding the reliability of critical infrastructure.

Supply Chain and Vendor Assurance

Horizon 2 places emphasis on managing foreign ownership and supply chain risks. FireBreak supports this by ensuring sensitive systems remain disconnected from untrusted vendors' networks unless a connection is specifically authorised. This provides organisations with a straightforward method to demonstrate compliance and helps the government build confidence in critical supply chains.

Data Security and Privacy Alignment

Proposed reforms to data retention and privacy laws necessitate stronger measures to mitigate the exposure of sensitive information. By enforcing physical separation of backup systems and critical datasets, FireBreak supports data minimisation principles and provides an auditable safeguard against unauthorised access. This aligns with Horizon 2's objective of building trust through stronger privacy protections.

Emerging Technology Safeguards

The rapid development of AI, quantum technologies, and advanced communications introduces new risks that demand precise controls. FireBreak can be applied to isolate AI training environments or research facilities, ensuring connectivity occurs only when required. Horizon 2 should consider requiring an AI "kill switch" for critical systems, providing safe and accountable use of these technologies.

Integration into Standards and Certification

Partnerships with organisations such as the IoT Alliance, Standards Australia, and national cyber policy forums would enable hardware isolation to be integrated into certification schemes, regulatory frameworks, and educational programs. This would provide Australia with a tangible enforcement mechanism that complements existing standards, strengthens sovereign resilience, and demonstrates leadership in shaping future cybersecurity norms.

Shield 3 – World-class threat sharing and blocking

FireBreak can support the development of more effective national threat-sharing and blocking mechanisms by providing a physical enforcement layer to complement intelligence-driven responses.

Proactive Blocking (Q24–Q25)

When the Australian Signals Directorate (ASD) or the Australian Cyber Security Centre (ACSC) issues threat intelligence indicating imminent risk, FireBreak enables immediate disconnection of vulnerable systems. This reduces reliance on software patches or vendor interventions, supporting a faster response cycle.

Enhanced Threat Sharing (Q26–Q29)

FireBreak's connection and disconnection events can be shared with sector-specific Information Sharing and Analysis Centres

(ISACs). For industries without established ISACs, such as manufacturing or transport, FireBreak deployments could be aligned with the creation of new mechanisms supported by ACSC and industry regulators.

Crisis Preparedness (Q30)

In the event of a large-scale cyber incident or national security emergency, the Department of Home Affairs may mandate rapid isolation of critical systems. FireBreak provides a coordinated means to achieve this across multiple operators. Incorporating physical isolation into exercises run by ACSC or through critical infrastructure partnerships with AEMO, APRA, and other regulators.

Trust and Collaboration

Current threat-sharing arrangements are often viewed as limited. A stronger approach would involve government, industry, and academia collaborating to model cascading impacts across sectors. Connection-state data from FireBreak could feed into ACSC's Joint Cyber Security Centres (JCSCs) and enhance sector readiness. This would complement "clean pipes" initiatives led by telecommunications providers under guidance from the Australian Communications and Media Authority (ACMA).

Shield 4 – Protected critical infrastructure

The discussion paper calls for a more mature SOCI Act framework and centralised risk management. FireBreak contributes by giving operators a clear and auditable means of enforcing physical isolation.

Regulatory Compliance

Under the SOCI Act, responsible entities are required to maintain risk management programs. FireBreak provides verifiable records of when systems are connected or disconnected, supporting compliance with these requirements and demonstrating timely containment for incident reporting.

Sector-Specific Standards

FireBreak enforces practices consistent with ACSC's Security by Design guidance, including multi-factor authentication, hardened device settings, and strict connectivity windows. This ensures that operators of critical systems cannot reduce protections in a way that introduces remote access risks.

Independent Audits

Auditors and regulators, including the Critical Infrastructure Centre within the Department of Home Affairs, should assess whether physical segmentation controls are in place. FireBreak's records provide evidence that isolation policies are being enforced in practice.

Graduated Protections for OT Networks

Government guidance should distinguish between IT-grade, classified-grade, and engineering-grade protections based on the consequences of failure. For the most critical OT networks, where compromise could result in mass casualties or environmental harm, the guidance should encourage the use of unidirectional gateways or hardware-enforced isolation. FireBreak offers a flexible alternative to fixed data diodes where two-way but controlled connectivity is required, allowing regulators such as AEMO or state-based safety authorities to apply context-specific standards.

Reducing Compliance Burden

Submissions from industry, including AGL, have cautioned against extending SOCI obligations indiscriminately. Clarifying definitions of critical data and consolidating reporting obligations would simplify the process. FireBreak assists organisations in meeting these refined requirements without additional operational burden.

Shield 5 – Sovereign capabilities

Developing sovereign cybersecurity capabilities requires collaboration among industry, academia, and government. FireBreak can support this by building skills, stimulating local research, and creating opportunities for Australian industry engagement.

Workforce and Skills (Q39–Q41)

Deploying and operating hardware-based isolation requires a blend of cyber, engineering, and operational skills. FireBreak

can be incorporated into training programs supported by the Cyber Skills Partnership Innovation Fund and through partnerships with universities to build capacity across Australia's workforce.

Research and Collaboration (Q42–Q43)
Academic institutions, particularly those engaged in AI, quantum, and OT security research, can use FireBreak to test isolation strategies. This collaboration would contribute to practical research outputs that support government objectives under Horizon 2.

Sovereign Capability Development (Q44–Q46)
While FireBreak itself is not manufactured in Australia, its integration into Australian systems provides opportunities for local companies to deliver installation, integration, and lifecycle support. Procurement policies could encourage Australian firms to develop complementary components and services, thereby strengthening sovereign supply chains and building national capability.

Shield 6 – Strong Regional and Global Leadership

Australia can demonstrate leadership internationally by embedding hardware-enforced isolation into domestic policy and advocating for its adoption across the region.

Cyber Diplomacy and Deterrence (Q46–Q50)
Including physical isolation in domestic standards and promoting its value in international forums would position Australia as a credible advocate for practical controls. Sharing expertise with Pacific and Southeast Asian partners through Department of Foreign Affairs and Trade (DFAT) cyber capacity-building programs would strengthen resilience across the region.

Standardisation and Alignment
Aligning isolation requirements with frameworks such as the EU NIS 2 Directive and the UK Cyber Security and Resilience Framework would demonstrate compatibility with established global best practices. This alignment could inform emerging international norms and reinforce support for a rules-based approach to cyberspace governance.

Regional Cooperation
Through existing partnerships, including the Quad, AUKUS, and ASEAN forums, Australia can lead by example in applying hardware-enforced isolation. Promoting its adoption across Indo-Pacific critical infrastructure sectors would both improve resilience and demonstrate Australia's commitment to advancing shared security interests.

Technology Overview and Innovation

FireBreak is designed to give organisations reliable control over when and how their systems are connected. Unlike software-based solutions, it utilises a hardware mechanism to open or close connections physically. When a connection is switched off, there is no pathway left in place, reducing the risk of unauthorised access.
The system allows for both disconnection and controlled two-way communication. This means it can support operational needs that require data exchange, while still enabling complete isolation when that is the safer option.

Changes to connection states are protected through multi-factor authentication and a permission structure, ensuring that only authorised personnel can adjust. Policies can be set so that connections are established or closed according to defined rules or schedules, giving organisations predictable and consistent control.

Management of FireBreak is carried out through a separate environment, independent from the data or operational network. This ensures that the device can still be managed if the primary environment is unavailable or compromised. Remote access options, such as a secure web interface or SMS commands, provide additional resilience for administrators.

FireBreak can be integrated into monitoring and response processes, allowing for automatic physical disconnection if unusual activity or a potential threat is detected. Manual overrides are also available, ensuring control always remains with the organisation.

Connectivity can be scheduled or activated only when required, for example, during backup processes, maintenance, or in response to equipment alerts. This approach reduces unnecessary exposure by ensuring systems are connected only for specific, defined purposes.

Taken together, these features make FireBreak a practical tool for organisations that need assured control of their critical systems. It supports day-to-day operations while maintaining clear safeguards against unwanted access.

Use-Case Library and Case Studies

The following examples illustrate FireBreak's applicability across sectors.

Healthcare and Enterprise – Ransomware Containment

In hospitals and large enterprises, ransomware outbreaks pose significant risks to safety and service continuity. FireBreak enables immediate disconnection of affected machines, preventing malware from reaching critical medical devices or business systems. Backup environments remain physically isolated until required for restoration, ensuring data integrity and supporting recovery efforts.

Finance – Backup and Recovery Protection

Financial institutions rely on backup and recovery environments to ensure business continuity. By scheduling FireBreak to disconnect off-site backup systems during normal operating hours, organisations limit exposure to remote attacks. In a crisis, the backup can be reconnected to restore data and then returned to a disconnected state. This reduces vulnerability while preserving reliable recovery capability.

Energy and Transport – OT Network Protection

Operators of power grids and transport networks face ongoing challenges in managing the interface between IT and operational technology (OT). FireBreak provides a physical layer of control, allowing operators to connect when adjustments to control parameters are needed and then disconnect once complete. This ensures secure, time-bound access without leaving persistent pathways open for exploitation.

Defence and Research – AI Training Isolation

Organisations developing artificial intelligence models for defence or research need to protect sensitive datasets and training environments. FireBreak enables these clusters to remain physically disconnected except during defined training periods. By connecting only when data is being processed, the risk of theft or sabotage is reduced, preserving the integrity of critical research assets.

Telecommunications – AI Outbreak Containment

Telecommunications providers are increasingly dependent on AI-driven systems for functions such as fraud detection. If an AI platform begins to behave abnormally, FireBreak can isolate it from the wider network immediately. This prevents interference with core systems and limits the risk of operational disruption.

Utilities and Remote OT Sites – On-Demand Connectivity

Water utilities, electricity networks, and renewable energy operators often manage geographically remote sites such as pumping stations, substations, solar farms, wind turbines, or hydro facilities. FireBreak ensures these sites remain disconnected by default, with connectivity enabled only when needed. If a sensor detects a fault or abnormal reading, FireBreak establishes a temporary connection to transmit diagnostic data to engineers before automatically disconnecting again. This approach minimises the attack surface while maintaining operational visibility across distributed OT environments.

Benefits and Metrics

The adoption of FireBreak provides clear and measurable benefits for Australia's critical infrastructure. By enabling physical isolation within seconds, FireBreak significantly shortens incident response times, reducing mean time to contain from hours to minutes and preventing lateral spread across networks. This capability directly supports compliance with 24-hour reporting requirements and helps operators demonstrate early containment during audits or investigations.

Equally important, information systems that do not require permanent connectivity can remain physically disconnected until needed. This reduces their exposure window by more than 90%, effectively bringing the attack surface for these assets to nearly zero. For critical sectors such as energy, water, transport, and health, this translates into fewer entry points for attackers and a measurable reduction in operational risk.

The presence of hardware-enforced isolation also represents a concrete risk-mitigation measure, which may be reflected in more favourable insurance and assurance frameworks. At a national level, FireBreak enhances trust in essential services by showing that systems can be reliably disconnected when threatened. These benefits align directly with Horizon 2's objectives of safeguarding critical infrastructure, strengthening citizen confidence, and ensuring Australia is seen internationally as a leader in practical cybersecurity capability.

Implementation Pathways and Recommendations

To support Australia's ambition to lead in cybersecurity, a set of practical policy measures can be implemented to embed hardware-enforced isolation as a baseline capability for critical infrastructure. These measures strike a balance between regulatory requirements and industry support, ensuring adoption across both large and small organisations. The following actions are proposed:

Inclusion in baseline standards

Relevant standards, such as the Australian Government Information Security Manual and SOCI Act regulations, should be amended to require physical isolation controls for designated critical functions. Standards should explicitly recognise out-of-band management mechanisms as a secure and reliable practice.

Grants and incentives

Introduce funding programs that help small and medium-sized enterprises adopt hardware-based segmentation. Subsidies could cover the cost of out-of-band management infrastructure such as dedicated control ports or cellular modules. Access to incentives should be tied to measurable reductions in incidents and demonstrated compliance with reporting timelines.

Pilot and certification programs

Run pilot projects in priority sectors to confirm the operational benefits of hardware isolation and refine deployment models. Establish a certification framework for devices that meet government-approved hardware security criteria, including secure out-of-band management and adherence to recognised interface standards.

AI kill-switch mandates

Artificial intelligence systems deployed in critical infrastructure require a physical disconnect mechanism that can prevent unintended or unsafe interactions with operational networks. Guidance should cover both automated triggers through monitoring platforms and manual overrides through secure channels such as SMS or API.

Sovereign manufacturing

Encourage domestic production and assembly of isolation devices by applying procurement policies that favour local suppliers. Industry development grants should be used to support Australian manufacturers in producing key components such as relay modules and control boards, building a sustainable sovereign capability.

Conclusion

The Horizon 2 consultation is an opportunity for Australia to define itself as a global leader in cybersecurity. Achieving this will not come from repeating existing strategies but by adopting bold, practical innovations that change the way critical infrastructure is secured. Goldilock's FireBreak platform represents such an approach. Built on the principle of "*Disconnect to Protect – On Demand*", it addresses a gap in current policy by introducing hardware-enforced physical isolation as a national capability.

By incorporating FireBreak into Horizon 2 initiatives, Australia can demonstrate to the world that it is prepared to lead with new models of resilience. This would protect critical infrastructure, provide businesses and citizens with greater assurance, and support the development of sovereign capabilities in advanced security technologies.

We welcome the opportunity to work with the Department of Home Affairs and other stakeholders to bring this vision into practice. Please direct enquiries to [redacted]