**Providing the following comment in response to the Australian Government Policy presentation on Horizon 2 and development of the Australian Cyber Security Strategy 2023-2030.**

**Premise:** To achieve the objectives of Shields 1-4 within months and within current budget restraints, we strongly advocate the Australian Government review and leverage best of breed commercial Cyber Open-Source Intelligence (OSINT) and Publicly Available Information (PAI) automated datasets, AI/ML analytics and continuous reporting to provide continuous awareness and actionable risk mitigation priorities across all AU Critical Infrastructure Sectors. This approach would leverage a proven practice used today in the financial sector with credit monitoring and reporting across all legal companies and organizations globally, providing best insights and practices for fighting identity theft and credit protection.

By incorporating this risk intelligence and awareness model mapped to the Australian Essential 8, the Australian Government can focus on analysis of metrics and threat trends that will enable achievement of Shields 5 and 6 in a within a year. Additionally, by integrating cyber risk to resilience experiential learning models and proven cloud-based platforms, the nation's secondary schools and higher education can provide access to the cyber monitoring data across critical infrastructure and key industries by Sector, Sub-Sector, Region and Size.

In this way the Australian Government could advance the skillsets and leverage the manpower of thousands of students while providing them with the awareness of digital risks and actions taken to reduce continuously mitigate vulnerabilities in their personal and professional behaviors. This would enable the National, Provincial, Local and Tribal Governments to conduct assessments and analysis of these sectors across all three levels of Information (Status, Capabilities, and Considerations) that would rapidly identify and disseminate across all sectors changes across the cyber ecosystem that identify threats, risks, mitigations, and metrics for developing proactive counters and rapid recovery of cyber incidents. Appendix A provides a breakdown of the three levels, the intended training targets, and training objectives of a cyber educational initiative currently being implemented by 5 US Universities.

**The integration and tailoring of best of breed commercial Cyber Risk/Threat monitoring, prioritization and mitigation cloud-based platforms can be provided as a scalable service of common concern, across any Critical Infrastructure (CI) Sector within 90 days, thereby systemically raising their resilience.**

**Executive Summary:** All CI Sector Entities remain top targets from a range of highly sophisticated, motivated State and Criminal Actors, due primarily to their many vulnerabilities and valuable datasets.

These same companies and organizations vary in size, cyber expertise, talent and resources, creating inequities and disparities in resilience, performance and assurance. Current approaches and controls to identify Cyber Risks, Threats and Vulnerabilities, are based primarily on self-assessments, best practices and industry standards such as the NIST Framework, ISSO, C2M2, CIS, CMMC, etc.- foundational but not sufficient to ensure Operational Assurance and Systemic Resilience continuously.

While CI Sector entities are generally cognizant of current cyber threats and methods, the majority do not have in-house cyber expertise and budgets to expeditiously identify, prioritize and effectively mitigate their top Cyber Risks continuously vs primarily responding to annual standards-based self-assessment audits and compliance. As a result, a majority of Financial/CI Sector companies and organizations have not advanced their resilience to online crime, fraud and disruption, in a way that can be continuously measured with real metrics on risk, maturity and compliance.

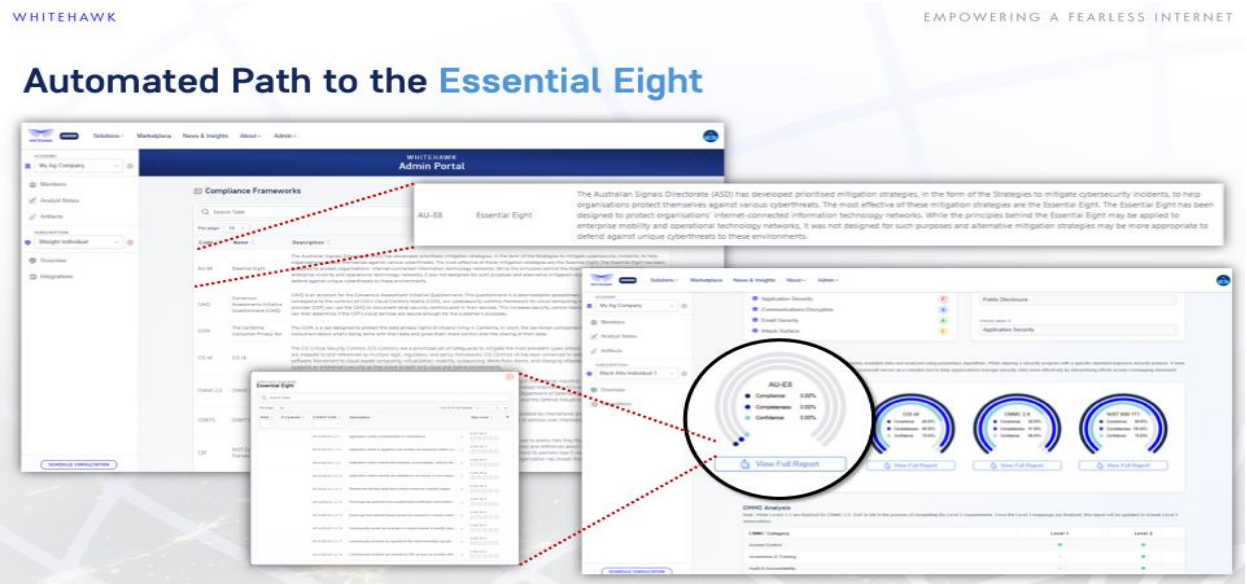
**With the advent of and access to publicly available network and global risk datasets, Software as a Service (SaaS) based instrumentation and Artificial Intelligence (AI) driven analytics, there are proven AU commercial risk and threat monitoring and alerting capabilities that can be leveraged externally, providing effective and timely Cyber Risk transparency and prioritization. Vetted and tested risk mitigation policies and solutions can then be reviewed and purchased via a CI Sector cloud based Cyber Marketplace.**

## CI Sector online Cyber Risk Platform and Service of Common Concern

### Key Commercial Cyber Risk Platform Features Include:

- ✓ **Risk Research and Discovery** — Collect, analyze, and correlate openly available data into actionable intelligence.
- ✓ **Continuous Risk Monitoring and Alerts** — Understand an organization's security performance, alerting to key changes.

- ✓ **Focused Automated Analytics** — Perform deep dives in areas that need focus rather than into the entire dataset.
- ✓ **Portfolio Trend Assessments** — Determine risk and threat trends impacting a Sub-Sector, Region or SMB population.
- ✓ **Ecosystem Maps** — Visualize the enterprise by understanding critical supplier and vendor interconnections and dependencies.
- ✓ **Compatible with Commercial API's** — Continuously vet and integrate with best of breed publicly available global risk and threat analytics.
- ✓ **Dark Web and Threat Insights** – Collect data from Dark Web forums for more complete datasets and situational awareness.
- ✓ **Mapping to NIST, ISSO, & 83 other Risk & Maturity Frameworks'**— Prioritize compliance, risk mitigation and business actions.
- ✓ **Integration Into an Automated Risk Management SaaS Dashboard** —near real-time stake holder review and management, with mapped regulations, alerts, artifacts, tasks and engagement.
- ✓ **Financial and CI Sector Curated IT/Cyber Marketplace**— As risk mitigation and best practice solutions and services are vetted, they can be onboarded into a cloud-based Marketplace where options are mapped to their respective maturity/risks/compliance needs and all solution Software Bill of Materials (SBOM) can be tested and monitored.



**Strategy: Critical Infrastructure Cyber Risk Service of Common Concern**

**Currently a majority of CI Organizations are working to stand up comprehensive and automated Cyber Risk programs with varying levels of resources.**
**Key Assumptions:**

- Critical Infrastructure efforts vary in effectiveness, scalability and expertise.
- Over the past decade, the commercial and academic sectors have invested billions of dollars in Software and Platform as a Service Cyber Risk Solutions, Acquisition of Globally available datasets and APIs.
- Many CI Entities contract with the same suppliers and contractors.
- It is easy to continuously vet, leverage, tailor, integrate and optimize best of breed commercial solutions to meet Cyber Risk specific mission and business objectives.
- Cyber Risk PaaS can be implemented and tailored within 30-45 days, loaded with tens of thousand's companies/organizations, simply with a CSV file of Supplier/Contractor legal names and URLs.

**Today's Proven Commercial Capabilities Include:**

**Advanced Predictive Analytics:** By fully leveraging Machine Learning and advanced Artificial Intelligence (AI) analytics across all publicly available datasets, organizations can identify the factors and behaviors that have the greatest probability of leading to unauthorized access and compromise. Analysis of vulnerabilities and risks across the end-to-end supply chain, identifies those vendors and suppliers that engage in risky sourcing and delivery of products and services with counterfeiting, tampering or flaws in hardware or software. With a Critical Infrastructure service of Common Concern that monitors thousands of companies globally, the platform analytics advance, providing key risk trend insights by Sector, Sub-Sector, Region, and Size, advancing predictability, indications and warning across key risk categories such as:

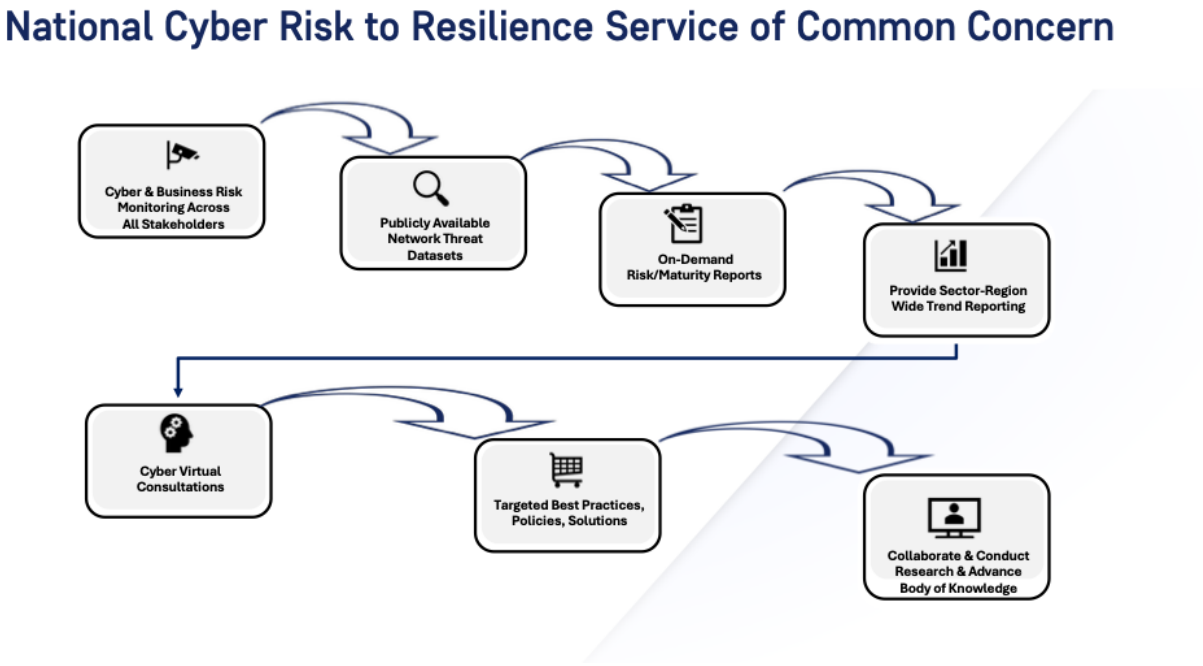
- Cyber Risk and Threat
- Maturity and Compliance
- Supplier Weaknesses and Supply Chain Saturation
- Open-Source Software Dependencies

**Continuous Vetting of New Cyber Risk global dataset and analytics' providers:** By continuously researching and vetting innovative technologies and providers, the platform stays current with changes in the environment at the speed of innovation. This vendor agnostic approach leveraging API and Data Integration enables a comprehensive view of risks and vulnerabilities.

**Critical Infrastructure Risk Management Framework:** When implemented at scale, the Cyber Risk Radar SaaS platform can monitor and share insights, measures and metrics across all Private companies and Public Sector organizations and their key Suppliers and Contractors, thereby identifying key vulnerabilities and threats impacting

suppliers or sector wide trends that must be mitigated at the organizational level, in order to drive sector resiliency to include:

- Systemically inform procurement and resilience decisions
- Prevent cyber events and warn of Industry/Sector wide vulnerabilities
- Identify risk factors that should be remediated by suppliers
- Highlight critical software dependencies and source code flaws
- ITAR/DFAR Section 889 restricted suppliers
- Foreign Influence/Control of sub-tier vendors and suppliers.




**CI Cloud Based Risk Mitigation Focused Marketplaces:** Link a Critical Infrastructure Cyber Resilience Program and Platform to a CI Sector sponsored Cybersecurity Marketplace of vetted vendors/suppliers/services. Then as desired CI Sector Entities can input their maturity, compliance, risk and SOC-2 datasets and shop based upon risk mitigation and capability gap priorities. Approach can include:

- Online interactive accounts with Cyber Threat Readiness, Maturity Profile and Risk Mitigation Virtual Consultations
- Automated & Documented Cyber Risk Prioritization, Maturity, Compliance and initial Action Plan matched to vetted, tested and monitored Solution Options
- Ability to seamlessly incorporate additional features to meet any operational requirements
- Tailored Marketplace Platform IOC can be implemented within 90 days based upon proven CI Sector lessons learned.

**The Critical Infrastructure Framework Value Proposition:**

1. **Who benefits directly from this approach & implementation?**
    a. All Private/Public Sector Companies and Organizations with publicly facing IT infrastructure.
    b. All CI Operations and Procurement focused Leadership CSO/CRO/CIO/CISO Teams.
2. **How will this save them money/funding/resources?** Cyber breaches and Supply Chain disruptions cost tens of millions per major event in lost data, lost infrastructure, damage assessment and investigation time, effort, and revenue - not to mention mission and business operations impact.
3. **How will this save them time or create efficiencies?** By providing near real-time insight into cyber risk, vulnerability, events and trends by Sector, Sub-Sector, Region and Size through an integrated, automated, scalable, online platform and flexible risk management framework. Therefore, vulnerability mitigations can be planned and acted upon in advance, versus being the result of outside exploitation attempts or worse - breach remediation.
4. **Impact/benefit to other tasks/priorities/projects?**
    a. Additional protection from foreign adversaries, cyber terrorists, global criminals across all CI Sector Entities from a flexible solution and framework that exists today.
    b. Identification of greatest areas of risk to critical infrastructure for prioritization of resources and surveillance.
5. **Why this approach instead of a different one?** There is no comprehensive, automated, scalable approach to identifying, prioritizing, and mitigating risks across the CI Sectors. Nationally and globally, we are spending billions on many disparate programs that for the most part is not effective and don't scale.
6. **Downside or negative effects to address.** Australian Government will need to ensure all the Cyber Risk and Threat data, analytics and reporting is effectively shared, protected, and consistently acted upon.

## ANNEX A – Levels of Analysis for Cyber Education and Awareness to Support Shields 1-4 of the Australian Government Cyber Security Policy 2023-2030

### Level 1 Status (Baseline posture and status of current processes)

- Target
  - High School/Undergraduate looking to explore a career in cybersecurity and want something that touches many areas.
- Training
  - Platform Management of the platforms ability to enter companies to be assessed.
  - Training on generating findings reports for analysis and action plans for remediation.
  - Training on understanding FAIR Analysis and what cybersecurity areas impact the ratings.
  - Researching vulnerabilities and CVE/CVSS scoring and how to remediate vulnerabilities.
- Findings Analysis
  - Vulnerability Risk Assessment
  - Remediation Measures and a Plan of Actions & Milestones for security improvement
  - Frameworks and Control Measures Gap Analysis and Deficiencies
- Deliverables
  - Scorecards
  - Vulnerability findings
- End Product
  - Understanding of how cyber risks and vulnerabilities are discovered and assessed.
  - Ability to conduct research vulnerabilities identified from PAI and how to quantify the risks to an individual entity.
  - Ability to prioritize risks and identify remediations with the greatest return on investment for improving security and resiliency.

### Level 2 Capabilities (Understanding of gaps and what capabilities will enable security of multiple entities with the highest ROI for security and resiliency)

- Target
  - Undergraduates Interns in cybersecurity or risk management looking to engage with entities in a portfolio or industry sector to plan remediations and assess the impact of remediation measure through monitoring and performance changes.
- Training
  - Platform management of entity portfolios
- Deliverables

- Scorecards
- Vulnerability Reports
- Portfolio Reports
- POA&Ms

- Analysis
  - Understand the sector and entity specific risks and vulnerabilities impacting an organization.
  - Quantification and enumeration of gaps and a prioritized list of remediation actions to be implemented.
  - Ability to assess and evaluate the impact of remediation measures, control artifacts and metrics to improve the posture and resiliency of an organization.
  - Quantification of security metrics and understanding of the efficacy of metrics in predicting potential risks
- End Product
  - Portfolio reporting and monitoring across all sectors and demographics identifying common threats and risk trends.
  - Analysis of performance metrics for proactive mitigation and remediation success.
  - Improvement of data collection and reporting by monitoring and testing organizations for faster improvement of data collection and accuracy.

**Level 3 Considerations (Identification of policies, metrics, best practices and areas of strategic investment that would generate the greatest benefit to resiliency and security of sector or subsectors of critical infrastructure or activities)**

- Target
  - Experienced security practitioners and graduate students in cyber law, policies, risks, or intelligence fields
- Training
  - Platform analysis of portfolios and sector risk analysis
  - Intelligence reports on the impact and effectiveness of past incidents and incident response measures
  - Platform access to business risks and supply chain ecosystem data
- Platform Deliverables
  - Portfolio reports
  - Business risk reports
  - Threat intelligence reports
- Analysis
  - Understand the impact of non-IT business and operational risks of cybersecurity.

- Analysis of best practices common across portfolios, industries, or sectors that should be implemented as standards.
- Quantification of cyber risks at a regional or national level and analysis of the policies, metrics, and remediations that will have the greatest return on investment for security and resiliency.
- Identification of common gaps or risks in critical infrastructure sectors or their supply chains where government actions, investment or regulation would significantly improve security and resiliency.
- Analysis of the impacts of government policies, regulations or standards on government, commercial, and private industries and quantification of the effects government and commercial entities

▪ End Product

- Policy recommendation for government and trade associations on programs and actions to improve data sharing and adoption of best practices.
- Metrics analysis to identify the practices, mitigations, and capabilities with the greatest improvement in predicting or countering cyber incidents.
- Analysis of data sharing, training, and implementation of cyber awareness education and cyber workforce development.

**Link to White Paper of Australian Cyber Resilience Moonshot:**

**Whitehawk.com/academia**

**Submitted by** [redacted]

[redacted]

[redacted]