Forging a Sovereign Cyber Workforce from the Australian Veteran Community

Compiled by [redacted]

Executive Summary

This submission proposes the **Sovereign Cyber Plan (SCP)**—a national program to transition discharging Australian Defence Force (ADF) members and their families into the cybersecurity workforce.

Each year, 6000 ADF members leave the service, all with training in cyber security concepts, and the majority with a Government security clearance. Fundamentally, the SCP is about recouping the investment already made in Australian veterans and repurposing it to be focused on the cyber community.

The SCP directly supports the 2023–2030 Australian Cyber Security Strategy, with immediate alignment to Horizon 2 (2026–2028) to scale industry capacity and grow a diverse, professional, sovereign workforce.

What the SCP delivers. The SCP is a tripartite partnership between government, training providers and employers. It offers a phased pathway: (i) foundational training via the national TAFE network; (ii) competitive, open-tender specialist academies to build job-ready capability; and (iii) structured employer integration. Curriculum and assessment will be mapped to SFIA roles/levels and aligned to ACSC Essential Eight, ISM and PSPF expectations, with an annual ASD-informed review to maintain currency. References to validation (e.g. the 2022 SANS veteran pilot and comparable international programs) will be cited where used.

Who the SCP serves. The program prioritises former ADF members and ADF spouses, with targeted outreach to women, First Nations peoples, and regional/remote communities. Delivery will include at least one national virtual cohort annually, supported by wrap-around measures (mentoring, wellbeing supports, reasonable adjustments, and childcare/relocation bursaries). A security-clearance pathway will be developed with AGSVA to streamline revalidation and re-sponsorship while safeguarding privacy.

Creating sustained demand. To convert training into jobs, the SCP proposes a "Veteran Cyber Employment" procurement mechanism that is compliant with the Commonwealth Procurement Rules (CPRs) and informed by lessons from the Indigenous Procurement Policy. Design safeguards will include: narrowly defined, publicly reported exemptions; independent compliance audits with published results; clear legal definitions (e.g., veteran-owned SME = ≥51% ownership and control; "meaningful veteran employment" with minimum hours, training plans and market-aligned remuneration); non-interchangeable targets for (a) veteran employment and (b) subcontracting value

to certified veteran-owned SMEs; and proportionate penalties for non-compliance.

Funding and value for money. Implementation integrates existing levers—Fee-Free TAFE and employer wage subsidies—to reduce net public cost. A full business case will present net cost per graduate after offsets and quantify second-order benefits (recruitment and clearance savings, taxation uplift from higher earnings, reduced DVA outlays, and ADF retention effects attributable to spousal employment).

Immediate actions for Horizon 2, from 2026.

- Commission a 12-month pilot across two priority specialisations with hybrid/virtual delivery.
- Publish a procurement options paper and integrity framework (exemptions register, audit model, definitions, penalties).
- Secure MoUs with anchor employers (sponsored places, guaranteed interviews, paid placements).
- Establish a longitudinal Monitoring & Evaluation (M&E) framework and baseline data-sharing protocols.
- Publish the standards map (SFIA ↔ ACSC/ISM/PSPF ↔ certifications) and equity participation targets.

How success will be measured. Core KPIs: graduate employment at 3/6 months; retention at 12/24 months; wage progression; time-to-hire; employer satisfaction; clearance timeliness; and proportion of contract value to veteran-owned SMEs, disaggregated by cohort (spouses, women, First Nations, regional/remote).

Conclusion. The SCP is a strategic, fiscally responsible investment that builds sovereign cyber capability, addresses a critical skills constraint, and delivers meaningful post-service careers for those who have served—advancing national security, economic prosperity and social cohesion.

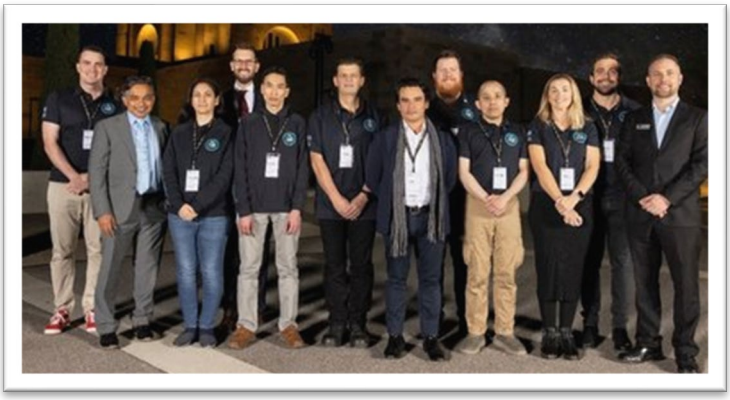


Figure 1 - Graduates of the 2022 Pilot Australian Veteran Cyber Academy

1. A Strategic Alignment with Australia's 2030 Cyber Vision

1.1. The Horizon 2 Imperative and Scaling the National Cyber Workforce

The 2023-2030 Australian Cyber Security Strategy sets a bold vision for Australia to become a world leader in cybersecurity by 2030. This vision is operationalised through a phased approach, with Horizon 2 (2026-2028) designated as the period to "Scale cyber maturity across the whole economy" by making "further investments in the broader cyber ecosystem, continuing to scale up our cyber industry and grow a diverse cyber workforce". The success of this critical phase is fundamentally dependent on the availability of a skilled and professionalised workforce.

This dependency is explicitly codified within the Strategy's architectural framework of six "cyber shields." While each shield provides a layer of defence, the efficacy of nearly all of them is contingent upon the success of **Shield 5: Sovereign Capabilities**. This shield's primary objective is to foster "a flourishing cyber industry, enabled by a diverse and professional cyber workforce". Without a sufficient pool of trained professionals, the goals of other shields, such as Shield 4, "Protected critical infrastructure," which requires experts to manage security obligations, or Shield 2, "Safe technology," which needs a workforce to embed secure-by-design principles, become unattainable. This structural interdependence means that a failure to deliver on the human capital requirements of Shield 5 represents a critical point of failure for the entire 2030 Strategy. Consequently, a dedicated and effective workforce development program is not merely a beneficial initiative but a foundational enabler for Australia's national security.

The Strategy itself, under **Initiative 17: Grow and professionalise our national cyber workforce**, acknowledges the scale of this challenge, identifying ongoing shortages, a lack of job-ready experience among entrants, and the need to transform the digital skills pipeline. This national-level assessment is strongly corroborated by submissions from industry leaders during the Strategy's consultation phase. PwC Australia identified "building a skilled and diverse cyber workforce" as a key area requiring significant focus, noting the persistent skills gap. Google highlighted the "global shortage of cybersecurity professionals" and advocated for public-private partnerships to create new career pathways. Similarly, EY Australia recommended "commensurate investment" in growing Australia's cyber security industry capacity and maturity. This broad consensus among government and industry underscores the urgency and strategic importance of implementing a robust, scalable, and targeted program to build the sovereign cyber workforce required to achieve the goals of Horizon 2.

1.2. The ADF Community: A Strategic National Asset for Cyber Defence

In the national search for a talent pool capable of meeting the demands of the cybersecurity sector, the discharging ADF community represents Australia's most strategically advantageous and underutilised human capital asset. The attributes developed and honed through military service align directly with the core requirements of a trusted cybersecurity professional. Beyond technical aptitude, these roles demand integrity, a disciplined approach to complex procedures, the ability to perform effectively under pressure, and an innate understanding of security principles. These are the foundational characteristics of ADF personnel, instilled through years of rigorous training and operational experience.

A significant and highly practical advantage offered by this cohort is in the realm of security clearances. The overwhelming majority of transitioning ADF members either hold a current security clearance or have held one recently. For Government and Commercial employers in the national security and defence industry sectors, this dramatically reduces the time, cost, and uncertainty associated with the vetting process, which can often be a major bottleneck in recruitment for sensitive roles.

This allows for the rapid onboarding of trusted individuals into high-priority positions, providing an immediate return on investment and accelerating the pace at which Australia can build its sovereign capability. The transition of these individuals should not be viewed as a cost to the national balance sheet, but rather as a strategic transfer of a national security asset from one domain of defence to another,from the kinetic to the digital.

Furthermore, the introduction of military veterans into the cybersecurity workforce addresses the Strategy's call for a "diverse cyber workforce" in a more profound way than is often considered. While diversity is rightly discussed in terms of gender and cultural background, the inclusion of veterans introduces a crucial element of cognitive diversity. Military training instils a unique and structured approach to planning, risk assessment, and incident response, often referred to as an "operational mindset." This framework, which prioritises mission objectives, contingency planning, and clear communication during a crisis, provides a valuable counterpoint to purely technical problem-solving. Integrating this operational mindset into corporate and government cyber defence teams can foster more robust and resilient security postures, moving beyond reactive technical fixes to holistic, mission-oriented defence strategies. This form of experiential diversity is a force multiplier, enhancing the collective capability of any security team it joins.

2. The Untapped Cohort: Quantifying the Opportunity in ADF Veterans and Families

2.1. The Annual Transition Flow, A Sustainable Talent Pipeline

The opportunity presented by the ADF community is not only one of quality but also of scale and sustainability. Each year, between 5,000 and 6,000 members transition from the Australian Defence Force, creating a consistent and predictable pipeline of high-calibre candidates for workforce development programs. This annual flow provides a renewable resource that can be systematically engaged to meet the growing demands of the cyber sector.

Demographic data from the Australian Bureau of Statistics (ABS) and the Australian Institute of Health and Welfare (AIHW) provides further context to this opportunity. A significant portion of the ex-serving population transitions at an age where they have decades of productive working life ahead. The ABS data from 2021 shows substantial numbers of previously serving members in the 25-34, 35-44, and 45-54 age brackets, representing individuals with a valuable combination of maturity, life experience, and a long career runway. This cohort is ideally positioned to undertake intensive reskilling and embark on a second career, offering employers a stable and mature workforce in contrast to the often-high turnover rates associated with younger, less experienced employees. The sustained nature of this transition flow ensures that any investment in a dedicated training program will yield continuous returns, providing a long-term solution to Australia's chronic cyber skills shortage.

Fundamentally, it is about recouping the investment already made in Australian veterans and repurposing it to be focused on the cyber community.

2.2. The Force Multiplier and Empowering ADF Spouses for a Resilient Defence Community

A truly strategic approach to leveraging the ADF community must extend beyond the transitioning member to their family, particularly their spouse. The inclusion of spouses in the SCP is not a matter of social welfare but a core strategic enabler with direct benefits for ADF capability, retention, and national economic resilience. The military lifestyle, characterised by frequent relocations, often forces spouses to abandon career progression, leading to underemployment and financial instability. This is a significant source of stress for military families and a contributing factor in the decision of experienced personnel to leave the service.

The nature of cybersecurity work offers a powerful solution to this long-standing problem.

Many roles within the field, from security analysis and threat intelligence to compliance and governance, are highly conducive to remote or flexible work arrangements. By equipping ADF spouses with in-demand, high-value cybersecurity skills and certifications, the SCP provides them with a much more portable career. A spouse can continue their professional development and maintain meaningful, well-remunerated employment regardless of their partner's posting location.

This has profound second and third order effects. It enhances the financial resilience of the Defence family unit, reducing stress and improving overall wellbeing.

This, in turn, makes a military career a more viable and attractive long-term proposition, directly contributing to the retention of skilled and experienced ADF members. By investing in the careers of military spouses, the nation is making a direct investment in the stability and effectiveness of its current fighting force. It transforms a historical challenge for the ADF into a strategic advantage, creating a more resilient Defence community and simultaneously adding a new stream of motivated and capable professionals to the national cyber workforce.

2.3. Enhancing Diversity and Inclusivity

The SCP is fundamentally aligned with the Strategy's goal of creating a more "diverse cyber workforce". As of June 2024, women comprised 20.7% of the permanent ADF, a figure that, while showing progress, highlights a significant opportunity for targeted engagement. The program will actively seek to recruit female veterans and spouses, offering a clear pathway into a high-growth, flexible career. Furthermore, the program will establish partnerships with First Nations veteran support organisations to create dedicated recruitment streams, mirroring the demand-side model of the Indigenous Procurement Policy and ensuring the benefits of this initiative are shared equitably. By actively targeting these cohorts, the SCP will not only address the skills shortage but also enrich the cyber sector with a wider range of perspectives and experiences.

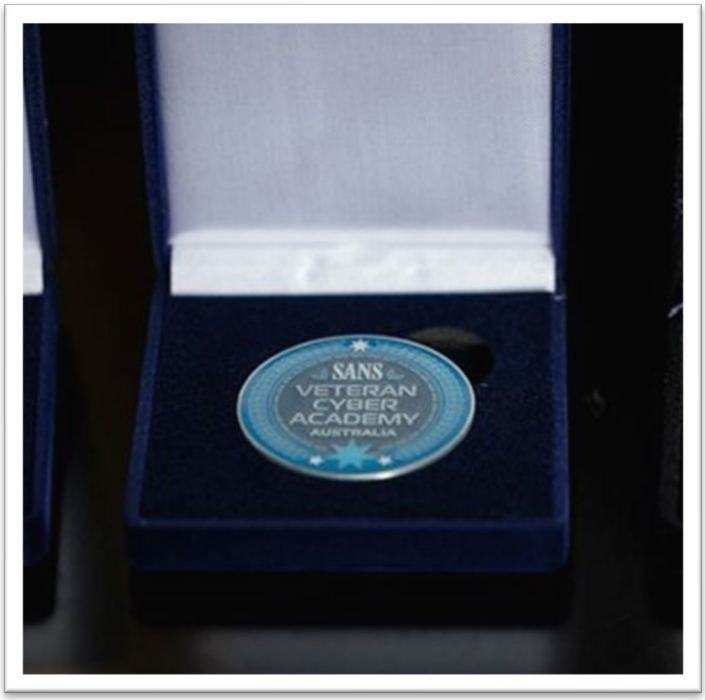
3. A Proven Pathway: The SANS Institute Pilot and International Best Practices

3.1. The Australian Proof-of-Concept and The 2022 Veteran Cyber Academy

The proposal for the SCP is not based on theoretical potential alone; it is grounded in the demonstrated success of a real-world Australian pilot program. In 2022, the SANS Institute delivered Australia's first Veteran Cyber Academy as a pilot program. This initiative graduated a cohort of 18 veterans and spouses of veterans, definitively proving that individuals from a diverse range of ADF backgrounds, many with no prior cybersecurity experience, can be rapidly and effectively reskilled to a job-ready, industry-certified

standard.

The key aspect of the academy wasn't the training; it was incorporating government and industry players. Upon graduation, trainees had their CVs reworked, received briefings from the Government and industry, and attended a careers fair. In the end, some students were offered employment even before graduation.



The structure of the pilot provides a robust template for a national program. It was a 16-week, intensive and immersive course that combined SANS' world-class training curriculum with practical, hands-on simulations and team exercises designed to replicate real-world scenarios. This focus on applied learning is critical, as it ensures graduates possess not just theoretical knowledge but demonstrable, practical capabilities. A key success factor was the integration of dedicated transition support and mentoring throughout the training.

The graduates of the 2022 academy achieved an average pass mark on all three exams of 85.74%, highlighting that this format and methodology produces high-quality, top-quintile cyber alumni.

Crucially, it facilitated direct engagement with potential government and private sector employers through organised career fairs, creating a clear and tangible pathway from the classroom to the workforce. The success of this pilot program in the Australian context serves as an invaluable proof-of-concept, mitigating the risk of a national rollout and

providing a validated model for curriculum, delivery, and industry integration.

3.2. International Benchmarking and Lessons from the US and UK

The long-standing and large-scale success of similar programs in allied nations further reinforces the success of the Australian pilot. These international examples demonstrate the model's scalability and provide valuable lessons for the design of a national Australian program.

In the United States, a mature ecosystem of support exists to transition veterans into cybersecurity careers. Programs like the VetSuccess Academy offer fully funded scholarships for advanced technical training and GIAC certifications.This is complemented by official government initiatives like the Department of Defense SkillBridge Program, which allows service members to undertake training and internships with industry partners during their final months of service while still on active duty. Furthermore, the Cybersecurity and Infrastructure Security Agency (CISA) runs a dedicated "Cybersecurity for Veterans" initiative, providing a comprehensive suite of resources, including career pathway tools, training catalogues, and information on funding mechanisms like the GI Bill. The key lesson from the US model is the deep integration of these programs into the official military transition process, creating a seamless and well-resourced pathway.

Similarly, the United Kingdom has developed a strong public-private partnership model. Programs like TechVets and the MoD & Veterans Cyber Academy provide a bridge for the Forces community into technology careers. These initiatives collaborate closely with industry bodies such as CREST and certification providers like CompTIA to offer a holistic package of free training, industry-recognised certifications, and extensive employment support, including CV distribution to over 190 partner companies. The UK model highlights the power of a community-based approach, leveraging veteran networks and strong industry partnerships to facilitate successful career transitions. These international precedents prove that the systematic transition of military veterans into cybersecurity is a recognised and effective national strategy for workforce development among Australia's closest allies.

3.3. Synthesising a Best-Practice Model for Australia

By synthesising the key success factors from the Australian pilot and these established international programs, a clear blueprint for a best-practice model emerges. This model is not just about delivering training content; it is about creating a comprehensive talent development pipeline that both candidates and employers trust.

The success of these programs reveals that they are not merely educational courses but powerful "brands" that signal quality to the market.

A graduate of a program like SANS VetSuccess or TechVets is a known quantity to employers, representing a pre-vetted, highly skilled, and reliable candidate. This branding effect is crucial as it de-risks the hiring decision for companies and creates a self-reinforcing cycle of employer demand and high-quality applicants. A primary objective for the SCP must therefore be to build and market the "Defence Cyber-Ready" brand as a hallmark of excellence within Australian industry.

The essential components of this best-practice model are:

1. **Aptitude-Based Selection:** Utilising validated assessment tools to identify candidates with the inherent aptitude to succeed in cybersecurity, ensuring that training resources are invested in those with the highest potential for success, irrespective of their prior technical experience.
2. **Accelerated, Immersive Training:** Employing intensive, "bootcamp" style delivery that focuses on practical, hands-on skills to rapidly move candidates to a job-ready state.
3. **Industry-Recognised Certifications:** Focusing the curriculum on achieving globally respected certifications from bodies like CompTIA and SANS (GIAC), as these credentials provide employers with a trusted and standardised measure of a candidate's knowledge and capabilities.
4. **Integrated Transition Support:** Embedding career services, professional mentorship, and direct employer networking as a core, non-negotiable component of the program from day one.
5. **Strong Public-Private Partnerships:** Building a collaborative delivery model where government provides strategic oversight and funding pathways, specialist providers deliver world-class training, and a consortium of employers commits to interviewing and hiring graduates.
6. **Competitive Neutrality:** Ensuring that specialist training providers for advanced stages are selected through open and competitive tender processes. This will prevent perceived favouritism, encourage participation from local Registered Training Organisations and universities, and help build Australia's sovereign training capacity.

4. The "Defence Cyber-Ready Program"

4.1. 4.1 Program Architecture: A Phased and scalable Approach

The proposed "Defence Cyber-Ready Program" is designed as a multi-stage, scalable framework capable of national implementation. Its architecture is specifically designed to

accommodate candidates with varying levels of prior experience, providing a broad and accessible entry point while also offering deep specialisation for those with the aptitude to excel. This phased approach ensures efficiency, allowing resources to be targeted effectively and providing multiple entry and exit points that align with both individual career goals and diverse industry needs. The program can be scaled to align with Horizon 2 timelines, with staged intake targets of 250 graduates in 2026, 750 in 2027, and 1,500 in 2028, subject to funding and demand.

4.2. 4.2 Stage 1: Foundational Skills Gateway (TAFE Partnership)

The first stage of the program serves as a wide-funnel, accessible entry point for the entire ADF community cohort, including members with minimal prior IT experience. The primary objective is to provide a solid baseline of essential knowledge and skills, preparing candidates for more advanced training and ensuring a common standard of foundational competency across the program.

- **Delivery Partner:** The national network of Technical and Further Education (TAFE) institutions is the ideal partner for this stage. TAFEs have an extensive physical and digital footprint across Australia, a clear mandate for delivering vocational education and training (VET), and existing infrastructure to manage student enrolments and support. This partnership leverages a proven, publicly funded system, ensuring scalability and accessibility.
- **Curriculum:** The curriculum will be nationally consistent and focused on core IT and security principles. Key modules will include computer hardware and software fundamentals, networking concepts, basic security principles, and an introduction to threat landscapes.
- **Certification Outcome:** The gateway stage will culminate in candidates sitting for an industry-standard, globally recognised foundational certification. The **CompTIA Security+** certification is the ideal target for this stage. It is widely regarded as the benchmark for entry-level cybersecurity roles, validating the essential skills required for core security functions and serving as a prerequisite for many intermediate and advanced positions. This certification aligns with the skills and knowledge expectations of an Australian Qualifications Framework (AQF) Certificate IV level qualification.

4.3. Stage 2: Specialist Immersion Academies (Industry Leader Partnership)

Candidates who successfully complete Stage 1 and achieve their foundational certification, or who can demonstrate equivalent prior learning and aptitude, will be eligible to progress to Stage 2. This stage is designed to provide intensive, deep-skill training in high-demand cybersecurity specialisations, transforming competent generalists into job-ready specialists.

- **Delivery Partner:** This stage will be delivered in partnership with world-class, industry-leading training providers selected via an open tender process to ensure competitive neutrality and build sovereign training capacity.
- **Curriculum:** The academies will be structured as a series of 16-week, part-time immersive "bootcamps," each focused on a specific career pathway. The curriculum will be reviewed annually with input from the Australian Signals Directorate (ASD) to ensure it remains current and incorporates emerging trends, including skills related to AI/ML security and secure-by-design principles, aligning with Shield 2 of the national strategy. To ensure broad accessibility, at least one "virtual academy" cohort will be run each year for participants in regional and remote locations. Initial streams could include:
    - **Cyber Defence and SOC Operations:** Focusing on network monitoring, intrusion detection, and defensive tools.
    - **Incident Response and Digital Forensics:** Focusing on responding to breaches, malware analysis, and evidence collection.
    - **Penetration Testing and Ethical Hacking:** Focusing on offensive techniques to identify and remediate vulnerabilities.

- **Certification Outcome:** Each specialisation stream will prepare candidates for advanced, highly respected certifications that demonstrate practical, hands-on mastery.

4.4. Stage 3: Employer Integration and Mentorship

To ensure a seamless and successful transition from training to employment, Stage 3 is not a sequential step but a continuous process that runs in parallel with Stage 2. Its objective is to embed candidates within the professional cybersecurity community and connect them directly with hiring organisations.

- **Mechanism:** This stage will be facilitated through a formal consortium of industry and government employers who have made a public "Veteran Employment Commitment". This creates a dedicated pool of organisations actively seeking to hire program graduates. A key milestone for the program's first year will be to secure and publish formal Memoranda of Understanding (MoU) from at least 10 major defence and critical infrastructure employers.
- **Activities:** The integration process will be structured and multi-faceted, including:
    - **Formal Mentorship Program:** Each student will be paired with an experienced cybersecurity professional (ideally also a veteran) from a partner organisation to provide guidance, support, and industry insights.

- **Dedicated Career Fairs:** Exclusive networking events will be held for each graduating cohort, allowing students to engage directly with hiring managers from the employer consortium.
- **Transition Workshops:** Professional development workshops focused on translating military experience for civilian resumes, mastering technical interviews, and navigating corporate culture.
- **Work Placements/Internships:** Opportunities for paid work placements or internships with partner organisations in the final weeks of the program, providing invaluable real-world experience and a direct pathway to a permanent role.

Table 1 - Proposed Phased Curriculum of the Defence Cyber-Ready Program

Stage	**Duration**	**Core Topics/Modules**	**Key Delivery Partner**	**Target Certification (and indicative AQF alignment)**
Stage 1: Foundational Skills Gateway	12 Weeks (Part-time equivalent)	IT Fundamentals, Network Concepts, Security Principles, Threat Landscape, Risk Management.	TAFE Australia	CompTIA Security+ (Certificate IV equivalent)
Stage 2: Specialist Immersion Academies	16 Weeks (Full-time)	**Stream A (Cyber Defence):** Security Operations,	SANS Institute (or equivalent via open tender)	**Stream A:** GIAC Security Essentials (GSEC) **Stream B:**

		Intrusion Detection, Endpoint Security. **Stream B (Incident Response):** Malware Analysis, Digital Forensics, Threat Hunting.		GIAC Certified Incident Handler (GCIH) (Diploma/Advanced Diploma equivalent)
Stage 3: Employer Integration	Concurrent with Stage 2	Mentorship, CV & Interview Workshops, Career Fairs, Networking Events, Work Placements.	Employer Consortium	Direct Employment

4.5. Program Governance and Accountability

To ensure quality, transparency, and effective delivery, the SCP will be governed by a dedicated steering committee. It is proposed this committee be chaired by the Department of Home Affairs, with the Australian Signals Directorate (ASD) serving as the technical lead and the Department of Veterans' Affairs (DVA) acting as the primary liaison for the candidate cohort. The committee's responsibilities will include accrediting training providers, overseeing curriculum quality, monitoring outcomes against KPIs, and ensuring alignment with the national strategy.

5. Activating the Ecosystem the Integration with Government and Industry Levers

5.1. Leveraging Existing Support Infrastructure

A key strength of the SCP proposal is its design for cost-effectiveness and rapid implementation through the strategic integration of numerous existing government support programs. Rather than requiring the creation of a large, new bureaucratic

apparatus and funding pool, the program acts as a central coordinating node, intelligently connecting veterans and employers to the wealth of resources already available. This approach maximises the return on existing taxpayer investments and significantly lowers the barrier to implementation.

For individual candidates, the training pathway is supported by multiple funding streams. Stage 1, delivered through TAFE, can be accessed via the **Fee-Free TAFE** initiative, a joint federal and state government program designed to upskill Australians in priority sectors. Transitioning ADF members can also utilise funding from the **Defence Career Transition Training (CTT) Program** to cover course costs and associated expenses. Furthermore, the principles of the **Veteran Recognition of Prior Learning (RPL) – Tertiary Support Grant Program**, which provides funding to universities to recognise military skills, could be adapted and extended to VET providers like TAFE to streamline the pathway for veterans with relevant experience. The program will also complement existing grant programs such as the Cyber Security Skills Partnership Innovation Fund, which supports collaborations between industry and education providers.

For employers, a powerful set of financial incentives already exists to encourage the hiring of veterans. The national **Workforce Australia's wage subsidy program** can provide up to $10,000 to businesses that hire eligible individuals, directly offsetting the initial costs of employment. This is complemented by veteran-specific programs, such as the DVA's

Employer Incentive Scheme (EIS), which offers reimbursement of up to 75% of a veteran's gross wages for the first three months of employment. By creating a program that produces graduates who qualify for these schemes, the SCP makes hiring a veteran not only a strategic choice but also a financially astute one.

Table 2 - Alignment of Program with Existing Government Veteran Support Initiatives and Funding Streams

Stakeholder	Relevant Government Program/Initiative	Benefit to the SCP
Candidate (Veteran/Spouse)	Fee-Free TAFE	Provides subsidised access to Stage 1 (Foundational Skills Gateway) training at

		TAFE.
	Defence Career Transition Training (CTT) Program	Provides funding for eligible members to cover costs associated with Stage 1 and Stage 2 training.
	Veteran Recognition of Prior Learning (RPL) Grants	Framework can be adapted to provide credit for prior military experience, potentially accelerating the training pathway.
Training Provider (TAFE)	National Skills Agreement (NSA)	Provides the overarching federal-state funding mechanism for VET delivery in priority areas like technology and defence.
Employer	Workforce Australia Wage Subsidies	Provides up to $10,000 to offset the wage costs of hiring a program graduate.
	DVA Employer Incentive Scheme (EIS)	Provides reimbursement of up to 75% of gross wages for the first three months of employment for eligible veterans.
	State-Based Veteran Employment Programs	Offers additional, state-specific wage subsidies

		and employment support services.
Veteran-Owned SME	Supporting Veteran Owned Business Grant Program	Provides funding and support for program graduates who wish to start their own cybersecurity consultancy.

This matrix clearly illustrates that the SCP is designed not to reinvent the wheel, but to provide the axle that connects all the existing wheels of government support, creating a cohesive and efficient vehicle for veteran transition. This pragmatic approach makes the proposal highly achievable and fiscally responsible.

5.2. Creating Demand: A Veteran Cyber Procurement Policy

While supply-side interventions like training are essential, a truly sustainable workforce pipeline requires a strong and consistent source of demand. To guarantee the long-term success of the SCP and ensure its graduates have ample career opportunities, a powerful demand-side policy lever is proposed: the creation of a "Veteran Cyber Employment" requirement within government procurement rules.

This proposal is modelled directly on the **Indigenous Procurement Policy (IPP)**. Since its inception in 2015, the IPP has generated over $9.5 billion in contract opportunities for Indigenous businesses by establishing mandatory minimum requirements for Indigenous participation in large government contracts and allowing for direct procurement from Indigenous SMEs. This policy has demonstrated that the Commonwealth's significant purchasing power can be effectively used to stimulate economic development and create opportunities for specific cohorts.

A similar policy could be implemented for the cybersecurity and defence sectors. Major Commonwealth contracts, particularly those from the Department of Defence and other national security agencies for ICT and cyber services, could include a clause requiring tenderers to meet a minimum target for the employment of certified veteran cybersecurity professionals, such as graduates from the SCP. Alternatively, it could mandate that a certain percentage of the contract value be subcontracted to veteran-owned cybersecurity SMEs. This policy would create a powerful, market-driven incentive for the entire defence

and technology industry to actively partner with the program, sponsor students, and hire graduates. It would embed veteran employment into the business-as-usual operations of the sector, creating a sustainable demand loop that ensures the viability of the program for years to come and solidifies the pathway from military service into the heart of Australia's sovereign cyber capability.

5.3. Indicative Cost-Benefit Analysis

While the program leverages existing funding streams, a dedicated budget is required for the specialist training in Stage 2 and overall program coordination. An indicative cost model demonstrates the program's fiscal responsibility and high potential for return on investment.

Table 3 - Indicative Per-Participant Cost Model

Program Element	Estimated Cost (AUD)
Stage 1: Foundational Skills Gateway	$2,000 - $5,000 (Largely offset by Fee-Free TAFE and CTT)
Stage 2: Specialist Immersion Academies	$20,000 - $40,000[1]
Certifications (CompTIA & GIAC)	$1,500 - $2,500 [59]
Program Admin & Transition Support	$2,000
Total Indicative Cost per Participant	**$25,500 - $49,500**
[1] *Cost for Stage 2 is an estimate based on international equivalents for 16-week immersive programs and is subject to variation based on tender outcomes, inflation, and the final curriculum design. Local alternatives may offer different price points.*	

Based on the staged intake targets, the total annual program cost would scale from approximately 250 graduate for 1,500 graduates before reaching a steady state. The return on this investment is substantial. With average entry-level cyber analyst salaries ranging from $85,000 to $110,000, and senior roles exceeding $150,000, graduates become significant net taxpayers within their first year of employment.

For employers, the program mitigates significant costs associated with recruitment (often 20-30% of first-year salary) and security clearance processing. A detailed business case should include a sensitivity analysis modelling variables such as participant attrition, employment rates, and salary outcomes to demonstrate a range of potential ROI scenarios.

5.4. Stakeholder Engagement and Communications

A proactive engagement and communications plan is essential to the program's success. The "Defence Cyber-Ready" brand will be promoted through a multi-channel strategy, including the official Veterans' Employment Program website, targeted social media campaigns, and direct engagement at Defence transition seminars and industry events. Formal consultations will be established with ADF leadership, DVA, and a broad consortium of industry partners to ensure the program's curriculum and outcomes remain aligned with stakeholder needs. This will be supported by feedback loops, such as annual surveys of participants and employers, to drive continuous improvement.

6. Measuring Success and Managing Risk

6.1. Defining and Measuring Success

To ensure accountability and enable continuous improvement, the success of the SCP must be evaluated against a set of clear, measurable, and publicly reported Key Performance Indicators (KPIs). This data-driven approach will move beyond anecdotal success stories to provide a transparent assessment of the program's impact and return on investment. The data sources and KPIs will be reviewed annually to ensure their continued relevance.

Proposed KPIs for the program include:

- **Throughput and Quality:**
  - Annual number of candidates commencing Stage 1.
  - Annual number of graduates from Stage 2 Specialist Academies.
  - First-time pass rate for target certifications (e.g., CompTIA Security+, GIAC).
- **Employment Outcomes:**
  - Percentage of graduates employed in a cybersecurity role within 3 and 6 months of graduation.

    - Average starting salary of employed graduates.
    - Number of unique employers hiring program graduates.
- **Ecosystem Engagement:**
    - Number of active corporate and government partners in the employer consortium.
    - Number of mentorship pairings established and maintained.
    - Annual value of wage subsidies claimed by employers hiring graduates.
    - Stakeholder satisfaction score (from annual surveys of participants and employers).
- **Diversity and Inclusion:**
    - Percentage of program participants who identify as women.
    - Percentage of program participants who identify as First Nations peoples.

6.2. Risk Management and Mitigation

A proactive approach to risk management is critical for the successful implementation of a national program. The following table outlines key potential challenges and corresponding mitigation strategies.

Table 4 - Risk Management Matrix

Risk	Mitigation Strategy
Low Candidate Uptake: Insufficient interest from the ADF community due to competing transition priorities or lack of awareness.	Proactive marketing and communications plan targeting transitioning members and spouses via Defence seminars and support networks. Clear articulation of career outcomes, including high salary potential and job stability.
High Attrition / Variable Pass Rates: Candidates struggle with the intensity of the training, leading to dropouts or failure to achieve certification.	Robust aptitude-based pre-screening to select candidates with high potential for success. Provision of strong student support and mentorship. Offer flexible delivery options (e.g., online/hybrid) to accommodate diverse learning needs.
Regional Accessibility Barriers:	Stage 1 to be offered via TAFE's extensive

Candidates, particularly spouses in regional or remote posting locations, are unable to access training.	regional and online network. Stage 2 will include at least one dedicated "virtual academy" cohort each year to ensure equitable access for participants in locations such as Darwin and Townsville.
Insufficient Employer Demand: A mismatch between the number of graduates and available entry-level positions.	Primary mitigation is the "Veteran Cyber Employment" procurement policy to create structural demand. Continuous engagement with the employer consortium to align training streams with industry needs. Active marketing of wage subsidies to de-risk hiring for SMEs.
Security Clearance Delays: Graduates face delays in starting sensitive roles due to lengthy clearance processing times.	Prioritise candidates with current or recently lapsed (within 24 months) security clearances. Engage with the Australian Government Security Vetting Agency (AGSVA) to establish a streamlined revalidation process for program graduates, with a service-level target of 20 business days.
Curriculum Obsolescence: The training curriculum becomes outdated due to the rapid evolution of cyber threats (e.g., advancements in AI-driven attacks).	Implement an annual curriculum review process led by the Program Steering Committee, with mandatory technical input from ASD, to update training streams and ensure alignment with the evolving threat landscape and the Strategy's focus on secure-by-design (Shield 2).

6.3. A Trifecta of Returns: National, Economic, and Social

The comprehensive benefits of the SCP deliver a compelling return on investment that

extends across national security, economic prosperity, and social cohesion. It is a single initiative that addresses multiple, interconnected national challenges.

- **National Security:** The most direct return is a rapid and scalable increase in Australia's sovereign cyber workforce. By creating a reliable pipeline of vetted, trusted, and highly skilled professionals, the program directly strengthens the nation's resilience against cyber threats. It reduces our strategic dependence on foreign expertise for critical defence and infrastructure protection roles and ensures that the human capital developed through military service continues to contribute to the national interest long after transition. This program is a direct investment in the operational capability of Australia's "cyber shields."
- **Economic Prosperity:** The SCP addresses a critical skills shortage that is consistently identified by industry as a major constraint on the growth of Australia's digital economy.
  By supplying the skilled professionals needed to drive innovation and secure digital transformation, the program acts as an economic enabler. Furthermore, it transitions veterans and their spouses from potential reliance on government support into high-paying, high-demand careers, turning them into significant taxpayers and active contributors to national prosperity.
- **Social Cohesion & Defence Capability:** The program provides a tangible and meaningful pathway for veterans to continue their service to the nation in a new capacity. It offers a high-status, respected "second career" that honours their military experience and provides long-term financial security. For the broader Defence community, the empowerment of military spouses with portable, valuable careers strengthens the family unit, improves wellbeing, and addresses a key driver of attrition from the ADF. By actively promoting diversity and inclusion, the program ensures these benefits are accessible to all members of the Defence community.

  This creates a positive feedback loop for Defence itself. By showcasing a prestigious and well-supported transition pathway into a high-tech career, the ADF becomes a more attractive proposition for the next generation of tech-savvy recruits. This enhances the ADF's brand as a premier developer of human capital, ensuring that the SCP serves not only as an effective "exit ramp" from service but also as a compelling "on-ramp" for future talent, securing Australia's defence and cybersecurity capabilities for decades to come.

Appendix A: Implementation Roadmap

The following table outlines a high-level implementation roadmap for the SCP, aligned with the Horizon 2 timeline of the 2023-2030 Australian Cyber Security Strategy.

Table 5 - High-Level Implementation Roadmap (2026-2028)

Phase	Timeline	Key Activities	Primary Outcome
Phase 1: Program Establishment	Q1-Q3 2026	Establish Program Governance (Steering Committee). Finalise partnerships with TAFE network. Conduct open tender for Stage 2 training providers. Develop and launch "Defence Cyber-Ready" brand and communications plan. Secure initial MoUs from 10+ anchor employers.	Program infrastructure and partnerships in place for launch.
Phase 2: Pilot Cohort and Initial Rollout	Q4 2026 - Q4 2027	Launch first Stage 1 and Stage 2 cohorts (Target: 250 graduates in 2026). Establish mentorship program and hold first career fairs. Implement data collection for KPIs. Launch first annual "virtual academy"	Successful delivery of training to initial cohorts and validation of the operational model.

		cohort.	
Phase 3: Scaling and Optimisation	Q1 2028 - Q4 2028	Scale intake to meet annual targets (750 in 2027, 1,500 in 2028). Conduct first annual curriculum review with ASD. Publish first annual performance report. Initiate independent performance audit (end of Year 2).	Program operating at Scale, with established processes for continuous improvement and public accountability.
Phase 4: Steady State and Handover	Post-2028	Continue program delivery at a sustainable SCPIe. Integrate findings from independent audit. Transition to business-as-usual operations under the Horizon 3 framework of the National Cyber Security Strategy.	A sustainable, long-term talent pipeline for Australia's sovereign cyber workforce.