Defence Industry Leadership Program

DILP Research Paper

The Culture of Caution: Over-Compliance and Its Impact on Defence Innovation

Defence Industry Leadership Program

The Culture of Caution: Over-Compliance and Its Impact on Defence Innovation

Project Team

Scott Woollatt
Jois Castro Ramirez
Daniel Bryan
Glen Stevens
Celanie Meyer

Project Mentor

Glen Gallagher

Daniel Bryan
Lockheed Martin

Glen Stevens
Selentium Defence

Meet Our Team

Jois Castro Ramirez
ASC

Celanie Meyer
Ascent Pty Ltd

Scott Woollatt
MacTaggart Scott
Australia

Glen Gallagher
(Project Mentor)
Defence SA

Disclaimer

The contents of this research paper are the opinions and views of the authors based on the research conducted and do not necessarily represent the views of the authors' organisations, the interviewees, the interviewees' organisations, the Defence Industry Leadership Program (DILP) or the Defence Teaming Centre (DTC).

All acronyms and descriptions are contained within Appendix A to support clarification.

Acknowledgements

This research paper would not have been possible without the support and guidance provided by our project mentor, Glen Gallagher.

The project team is also extremely grateful for the support provided by over 40 defence industry experts who contributed to our research through both the industry survey and interview stages. We extend our sincere thanks to each contributor, including the following companies:

We also acknowledge a number of others who completed the survey anonymously, their contribution to our research is valued and we are grateful for their time.

The project team would also like to thank the DILP teams from both the Defence Teaming Centre and Skills Lab for their work in administering the DILP program and supporting DILP participants.

Contents

1. Executive Summary

Innovation underpins Australia's sovereign Defence capability, yet many small and medium enterprises (SMEs) experience Defence compliance frameworks as complex, inconsistent, and resource-intensive.

This study examined whether over-regulation and over-compliance are stifling innovation in Australian Defence SMEs, with a focus on two domains common to all Defence contracts - security and procurement.

A mixed-methods approach combined a national SME survey, comparisons to international systems, and targeted interviews with senior Defence and industry figures.

Across these data sources, a consistent pattern emerged: compliance systems designed to ensure safety and accountability have grown into barriers that delay or deter innovation.

SMEs described navigating overlapping frameworks - DISP, PSPF, ISM, Essential Eight, and ASDEFCON - each intended to build trust but collectively consuming time, money, and momentum.

From this, five recurring friction points underpinning culture between concept and capability were identified - Complexity, Caution, Compliance, Credibility, and Cost.

Together they describe a self-reinforcing cycle where Defence's intent to innovate is overtaken by its instinct to control: complexity drives caution, caution demands compliance, compliance erodes credibility, and cost justifies new complexity in controls.

The result is a system that protects process more than progress.

The analysis found that regulation itself is not the enemy of innovation, but its uniform, risk-blind application.

Defence's challenge is to retain assurance while restoring agility - to scale oversight to consequence rather than apply it indiscriminately.

To rebalance the system, this report recommends three practical reforms:

- **Refining ASCA's innovation pathways** – Define functional outcomes rather than specific products and create a second channel for high-quality unsolicited proposals;
- **Re-calibrating Defence Risk Appetite** – Shift from risk avoidance to risk management proportionate to consequence;
- **Simplify and Clarify Compliance Pathways** – Strengthen the Office of Defence Industry Support through a Defence Ready portal.

Collectively, these reforms would move Defence from a culture of protection to one of confident collaboration - where oversight enables innovation, compliance builds confidence, and Australia's industrial ingenuity becomes a true strategic advantage.

2. Introduction

2.1. Innovation in the Australian Defence Industry

Innovation within the Australian Defence Industry has become a central pillar of national capability and sovereign resilience. The Government's *Defence Industry Development Strategy* (Department of Defence 2024) and the establishment of the *Advanced Strategic Capabilities Accelerator* (ASCA) (Department of Defence 2023) demonstrate a clear intent to accelerate the development and adoption of homegrown technologies.

However, Australia's Defence innovation ecosystem remains shaped by complex regulatory, security, and procurement frameworks. These mechanisms ensure assurance, safety, and accountability but can also slow the transition of ideas into operational capability. For Small and Medium Enterprises (SMEs) - often the source of the most agile and disruptive ideas - navigating this environment can be particularly challenging. The balance between control and creativity has therefore become a defining tension within Australia's quest for sovereign innovation.

2.2. Problem Statement

This study addresses the question:

"The Culture of Caution: Over-Compliance and Its Impact on Defence Innovation"

While regulation is essential to protect national interests, excessive or inconsistent application can transform compliance from a framework of assurance into a barrier to progress. Many SMEs report that time, cost, and uncertainty associated with compliance obligations divert resources away from research and development, discourage participation in Defence procurement, and reduce their respective competitiveness. Unlike Primes who can shoulder the weight of the commercial burden - SME's suffer.

Understanding whether these frameworks enable or inhibit innovation is critical to ensuring that regulatory intent aligns with Defence's strategic goal: building a modern, agile, and innovative industrial base.

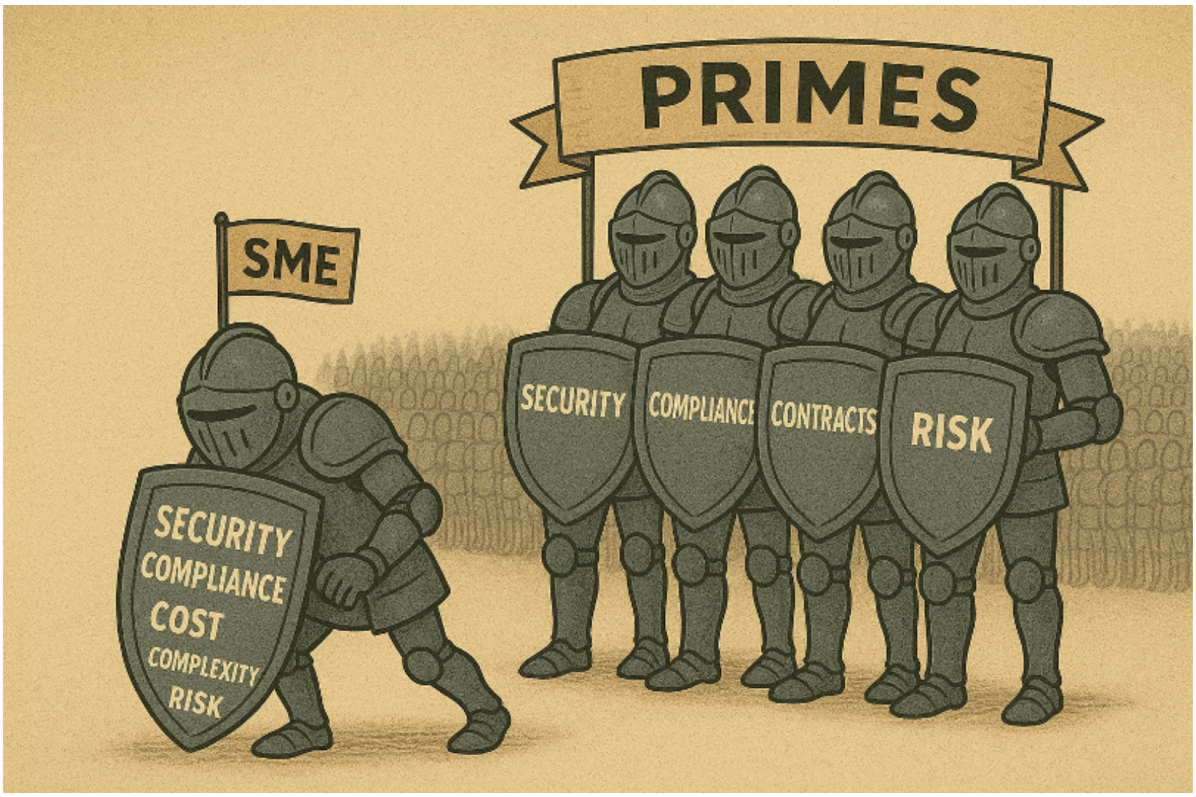


Figure 1 - Armour burdens SME's while Primes can shoulder the commercial weight

2.3. Research Focus

The study narrows its focus to two domains common to every Defence contract: security and procurement.

Security frameworks such as the *Defence Industry Security Program* (DISP), the *Protective Security Policy Framework* (PSPF), and the *Australian Government Information Security Manual* (ISM) establish the baseline for trust between Defence and industry. Procurement frameworks, particularly *ASDEFCON* and its derivatives, define how that trust is operationalised through contracts. Together, these systems represent both the entry gate and the operational environment for SMEs seeking to engage with Defence.

By examining these two perspectives, the research explores how regulatory design, administrative behaviour, and cultural factors combine to shape innovation outcomes across the Defence ecosystem.

2.4. Objectives

The objectives of this study are to:

- Identify how *over-compliance* and regulatory complexity affect the innovation capacity of Australian Defence SMEs;
- Analyse whether existing security and procurement frameworks enable or constrain innovative practices;
- Capture industry perspectives on the cultural and behavioural drivers of over-regulation within Defence;
- Develop evidence-based recommendations that promote proportionality, clarity, and accessibility in compliance; and
- Contribute to policy discussions on how Defence can balance assurance with agility in pursuit of sovereign capability.

2.5. Scope and Limitations

This research focuses on the lived experiences of Australian SMEs operating within the Defence supply chain. It concentrates on compliance and innovation issues linked to security and procurement frameworks rather than broader industrial policy or technical R&D performance. Data were collected through surveys, and targeted interviews, involving SMEs, Primes, and Defence representatives.

The findings reflect perceptions and experiences within a defined sample and timeframe (2024-2025) and are therefore interpretive rather than exhaustive. While the study identifies systemic trends and barriers, it does not evaluate specific Defence programs or individual compliance audits. Its purpose is diagnostic - to illuminate patterns and provide recommendations for proportional reform - rather than prescriptive in a legal or regulatory sense.

3. Defining Innovation

To frame this section of the report, we conducted a targeted interview with David Pender, whose extensive experience in organisational innovation provided a practical lens on how ideas are developed, tested, and adopted within complex systems such as Defence. His perspectives helped illuminate the cultural and behavioural dynamics that shape innovation beyond formal processes. To complement this, we reviewed a range of academic and peer-reviewed sources, including foundational works by Schumpeter, contemporary analyses in the OECD's *Oslo Manual*, and research exploring how regulation interacts with innovation in high-reliability sectors.

3.1. Types of innovation

Innovation is widely recognised as essential for competitiveness and capability, yet it is often defined in inconsistent ways. At its core, innovation is about turning ideas into value, whether that value is improved efficiency, new capabilities, or greater effectiveness in solving problems (OECD, 2018).

Scholars and practitioners commonly distinguish between different forms:

- Incremental innovation: small, continuous improvements. In Defence, this might involve refining an existing weapon system or making software slightly more efficient.
- Radical innovation: breakthroughs that fundamentally shift how things are done, such as the adoption of unmanned aerial vehicles.
- Product innovation: new or improved physical systems, equipment, or technologies.
- Process innovation: changes in the way activities are carried out, such as manufacturing, testing, or procurement methods.

Joseph Schumpeter (1934) described innovation as the "*new combination*" of existing knowledge, resources, or methods. This aligns with David Pender's observation that innovation is often less about entirely new inventions and more about reconfiguring what already exists to create new outcomes.

3.2. Innovation in Practice

In high-reliability sectors like Defence, incremental innovation is the norm because systems must be safe, tested, and proven before deployment (Abernathy & Utterback, 1978). Yet, Pender highlighted the tension between this culture of perfection and the potential of iterative, *Minimum Viable Products* (MVPs). He contrasted the Israeli Defence Force's rapid prototyping - "*build it, test it, learn, try again*" - with Australia's slower approach, where something as simple as a box of matches required the same introduction-into-service process as, for example, a missile. The result is that potentially useful innovation can be delayed until they lose relevance.

Process innovation can be just as transformative as product innovation. Pender shared an example from Singapore's shipbuilding industry, where animators were hired to model ship blocks virtually rather than building expensive steel prototypes. This process change saved time, reduced costs, and accelerated delivery. Such cases demonstrate that innovation is not confined to "*hard technology*" but can emerge from new ways of working.

Not all innovation is deliberate. History is full of accidental innovations, from pharmaceuticals being repurposed for uses other than what they were originally invented for, to unexpected discoveries in materials science. Pender noted that this type of "*serendipitous innovation*" requires systems that allow ideas to be tested in different contexts, rather than dismissed if they fail their first intended purpose.

Equally important is knowledge innovation. Pender argued that in Australia, innovation is often hampered not by lack of ideas but by poor knowledge sharing. Knowledge management is too often reduced to storing documents rather than building living systems of expertise that can be reused and recombined. This reflects broader literature emphasising ecosystems and collaboration as drivers of innovation (Dodgson et al., 2011).

3.3. Examples of innovation in Defence and other industries.

Table 1, below, summarises key types of innovation, drawing on both academic definitions and real-world Defence examples. This framing helps clarify how SMEs might experience innovation differently depending on whether they are improving existing processes, developing entirely new products, or navigating more accidental or knowledge-driven breakthroughs.

Table 1 - Key types of innovation

Type of Innovation	Definition	Example in Defence	Insight / Relevance
Incremental	Small, continuous improvements to existing products or processes	Refining an existing radar system to reduce weight and power use	Low-risk and common in Defence; helps maintain reliability but rarely shifts the game
Radical (or Disruptive)	Breakthrough changes that fundamentally alter practices or markets	Adoption of unmanned aerial systems instead of manned surveillance aircraft	Often resisted due to risk aversion and regulatory hurdles; requires cultural shift to iterative, MVP-style approaches

Type of Innovation	Definition	Example in Defence	Insight / Relevance
Product	New or significantly improved goods, technologies, or systems	Development of autonomous underwater vehicles	Tangible outputs are visible and easier to measure, but may struggle with acceptance in a single-buyer system
Process	New or improved methods of production, testing, delivery, or procurement	Singapore's use of digital animation to test ship blocks instead of building physical prototypes	Can dramatically cut costs and timelines; often overlooked compared to product-focused innovation
Planned	Innovation resulting from deliberate R&D programs or strategy	A Defence-funded program developing new cyber Defence tools	Requires strong pathways for commercialisation and adoption; often slowed by bureaucracy
Accidental	Unexpected discoveries or unintended applications	Pharmaceutical repurposing; in Defence, adapting commercial drone tech for battlefield use	Systems need flexibility to spot and harness these opportunities
Knowledge-based	Innovation through managing and sharing expertise across networks	Building collaborative industry databases instead of siloed document storage	Critical for SMEs, where access to shared knowledge can accelerate capability development

As the table highlights, innovation is multi-dimensional. In Defence, it is rarely a choice between one type and another; rather, SMEs often engage in several forms simultaneously, whether improving existing systems, experimenting with new technologies, or sharing expertise across networks. Recognising these different types is important because the impact of compliance and regulation will vary: what supports incremental product improvements may stifle radical or accidental breakthroughs, and what enables knowledge sharing may not support new hardware development. Understanding innovation in these terms sets the foundation for exploring how over-regulation or over-compliance might shape SME opportunities in the Australian Defence environment.

3.4. How regulation and compliance interact with innovation

The relationship between regulation and innovation is complex. Regulations are designed to ensure safety, quality, security, and accountability, all of which are critical in Defence. Yet they can also introduce rigidities that delay or discourage new approaches. Academic research often frames this tension as a "*double-edged sword*": regulation can be both an enabler and an inhibitor of innovation, depending on how it is designed and implemented.

Regulation as a Positive Force for Innovation

From a positive perspective, regulation can create clear standards and incentives that enable innovation. For example:

- **Level playing field:** Well-designed rules ensure all firms meet minimum requirements, which can build trust in new technologies (Blind, 2012). In Defence, cybersecurity standards or safety protocols provide confidence to buyers and users, which in turn encourages adoption of new solutions.
- **Market shaping:** Regulations can stimulate innovation by creating demand for solutions that meet new criteria (Ashford & Hall, 2011). Environmental regulation in automotive industries, for example, accelerated the development of cleaner technologies. By analogy, Defence SMEs may innovate in secure communications or data protection to meet new Defence security requirements.
- **Risk reduction:** Defence operates in high-stakes environments. Regulation provides assurance that innovations will not endanger personnel or capability. As David Pender noted, "*compliance systems that improve the safety of our war fighters make total sense*". In this way, compliance can be a foundation of trust rather than a barrier.

Regulation as a Constraint on Innovation

In contrast, regulation can also act as a barrier:

- **Cost and resource burden:** SMEs often lack the resources to meet extensive compliance demands. Excessive certification, auditing, and documentation requirements can divert scarce funds from research and development (Gans & Stern, 2003).
- **Time delays:** Lengthy approval and introduction-to-service processes can make innovations obsolete before they are deployed. Again, looking at the example where matches took six months to approve under the same process as weapons would. illustrating how disproportionate compliance slows even simple innovations.
- **Risk aversion:** Regulation can reinforce a culture of perfection and discourage iterative learning. In Australia, Defence has often prioritised "*perfect plans*" over minimum viable products, in contrast to Israel's rapid test-and-learn approach. This mindset stifles radical innovation by treating mistakes as failures rather than as learning opportunities.

Over-regulation vs over-compliance

Pender distinguished between necessary compliance for safety and over-regulation arising from risk aversion. For example, multiple re-inspections of imported components add cost without adding value. This reflects what scholars call "regulatory overreach," where rules multiply without proportional benefit (Coglianese, 2012).

Balancing the Two Sides

The academic literature suggests that the effects of regulation depend on its design. *Smart regulation* frameworks (Gunningham & Grabosky, 1998) emphasise proportionality, flexibility, and outcome-based standards rather than prescriptive rules. These allow firms to experiment with different solutions while still meeting safety and security goals. Similarly, theories of *adaptive regulation* argue that regulatory systems should evolve with technology and encourage iterative learning (Baldwin et al., 2012).

David Pender's comments align with these perspectives: he suggested that the problem in Australian Defence is not compliance itself, but a combination of risk-averse culture, single-buyer dynamics, and regulatory layering from successive reviews. In such an environment, compliance shifts from enabling trust to pushing risk down the supply chain, leaving SMEs overburdened with requirements they are ill-equipped to manage.

Implications for Defence SMEs

For SMEs, this tension is particularly acute:

- Regulation can open opportunities (e.g., developing cyber-resilient systems to meet Defence's security standards).
- At the same time, the cost and complexity of compliance can exclude SMEs from procurement processes or force them to partner with larger Primes, limiting their ability to innovate independently.
- The challenge is to design compliance regimes that protect defence personnel and national interests while leaving room for experimentation, iteration, and timely delivery of new ideas.

Theoretically, regulation and compliance should not be seen as inherently positive or negative, but as contextual levers that can either foster or suppress innovation. In the Defence SME sector, the stakes are high: rules that enable safety and trust can also unintentionally slow the very innovation they aim to protect. The key lies in proportionality, adaptability, and recognising that innovation requires both guardrails and freedom to experiment.

3.5. International comparisons

Australia is not unique in grappling with the tension between regulation and innovation in Defence. Other jurisdictions face the same challenge of ensuring safety, accountability, and security while enabling timely, effective innovation. What differs is how they structure their regulatory and procurement systems to achieve balance. A brief review of international approaches offers useful lessons for Australian Defence SMEs.

United States: Dual Pathways of Compliance and Innovation

In the United States, Defence acquisition has long been governed by a highly structured, compliance-driven regime under the *Federal Acquisition Regulation*. Recognising that this model could not respond quickly enough to modern operational demands, recent reforms have deliberately created a dual pathway for capability development. The Secretary of Defense's 2025 direction to transform the traditional Defense Acquisition System into the "*Warfighting Acquisition System*" explicitly prioritises speed, delegated authority, and mission-focused outcomes over procedural volume (US Department of Defense 2025a).

Parallel reforms to the Joint Requirements process mark an equally significant cultural shift. The disestablishment of JCIDS and the realignment of the Joint Requirements Oversight Council to focus on a short list of "Key Operational Problems" aim to close the gap between experimentation, requirements, and resourcing. New structures such as the *Requirements and Resourcing Alignment Board* and the *Joint Acceleration Reserve* are designed to ensure that proven innovations have a clear pathway into funded programs, rather than becoming trapped in pre-acquisition limbo (US Department of Defense 2025b).

A third reform effort targets the US arms-transfer and security-cooperation enterprise. By integrating disparate export and cooperation functions under acquisition leadership and modernising the supporting IT systems, the Department aims to reduce regulatory friction, improve responsiveness to allies, and better align industrial-base considerations with US and partner requirements (US Department of Defense 2025c).

These reforms illustrate a deliberate US effort to maintain robust oversight for major programs while creating faster, more flexible pathways for innovation. For Australia, this demonstrates that assurance and agility do not need to compete, provided the system is designed with differentiated routes that match the urgency, maturity, and risk of the capability in question.

Israel: Iteration and Minimum Viable Products

Israel is frequently cited as a leader in military innovation. The Israeli Defence Force (IDF) operates in a high-threat environment and has adopted an iterative, field-driven approach. innovations are tested rapidly in operational settings, often through Minimum Viable Products (MVPs). David Pender highlighted how the IDF will "take that minimum viable product, test it, come back and say that doesn't work, and then try again". Regulation in this context is flexible and outcome-oriented: the priority is speed and adaptability rather than exhaustive compliance upfront. The result is a culture where failure is treated as learning, not as a disqualifier.

Ukraine: Innovation Under Pressure

The war in Ukraine has created conditions for radical Defence innovation. With urgent battlefield needs, compliance and procurement rules have been loosened to enable direct, rapid purchasing by frontline commanders. Pender noted that officers with field responsibility can now order directly from suppliers, often tailoring products to immediate needs. This decentralised, demand-driven model shows how regulatory flexibility can unlock innovation under crisis conditions. While not sustainable in peacetime, it illustrates the importance of adaptability: strict compliance regimes that might work in stable contexts can be bypassed when urgency requires speed.

United Kingdom: Collaborative Standards and Ecosystems

The UK has moved toward embedding collaborative practices in procurement and contracting. Pender noted that suppliers in the UK Home Office context cannot secure contracts without certification to ISO 44001 (collaborative business relationship standard). This shifts compliance away from box-ticking and toward behavioural standards that foster trust and joint problem-solving across the supply chain. By treating innovation as an ecosystem-wide effort, the UK integrates compliance and innovation through a systems lens rather than placing the burden entirely on individual SMEs.

Singapore: Process Innovation and Pragmatism

Singapore provides an example of pragmatic process innovation. Pender described how, in maritime construction, firms reduced costs and delays by hiring animators to model ship components virtually, rather than waiting for expensive prototypes. This was enabled by a regulatory culture that supported practical experimentation with processes, provided safety and quality were maintained. Singapore also benefits from a strong government-industry partnership, where regulations are closely tied to national capability goals and adjusted as needed to sustain competitiveness.

Across these cases, several themes emerge:

- Flexibility and adaptability are critical. Israel and Ukraine demonstrate that fast iteration and decentralised decision-making can accelerate innovation.
- Dual pathways matter. The U.S. model shows that compliance-heavy systems can coexist with alternative contracting mechanisms that encourage SME participation.
- Collaboration as compliance. The UK illustrates how compliance requirements can be reframed to support ecosystem-wide behaviours rather than burdening single firms.
- Pragmatic process regulation. Singapore highlights that innovation is also about smarter ways of doing things, enabled by supportive regulatory culture.

For Australia, the lesson is clear: regulation should not be eliminated as it underpins safety and assurance. However, it must be proportionate, adaptive, and strategically designed to allow SMEs room to experiment and contribute. A single rigid compliance pathway risks stifling innovation; diversified and collaborative models can better balance the competing demands of assurance and agility

4. Methodology

Research on this topic was initially met with several regulatory frameworks for exploration and consideration. A tactical approach was taken to focus solely on two fundamental areas common to all Defence contracts: **security** and **procurement**. With scope defined, research was divided into 3 key phases:

- **Phase 1** - Understand and refine the topic
- **Phase 2** - Seek input and insight from experts in the Defence sector, and
- **Phase 3** - Analyse and document findings and recommendations

Each of the three phases is described in *Figure 2* below.

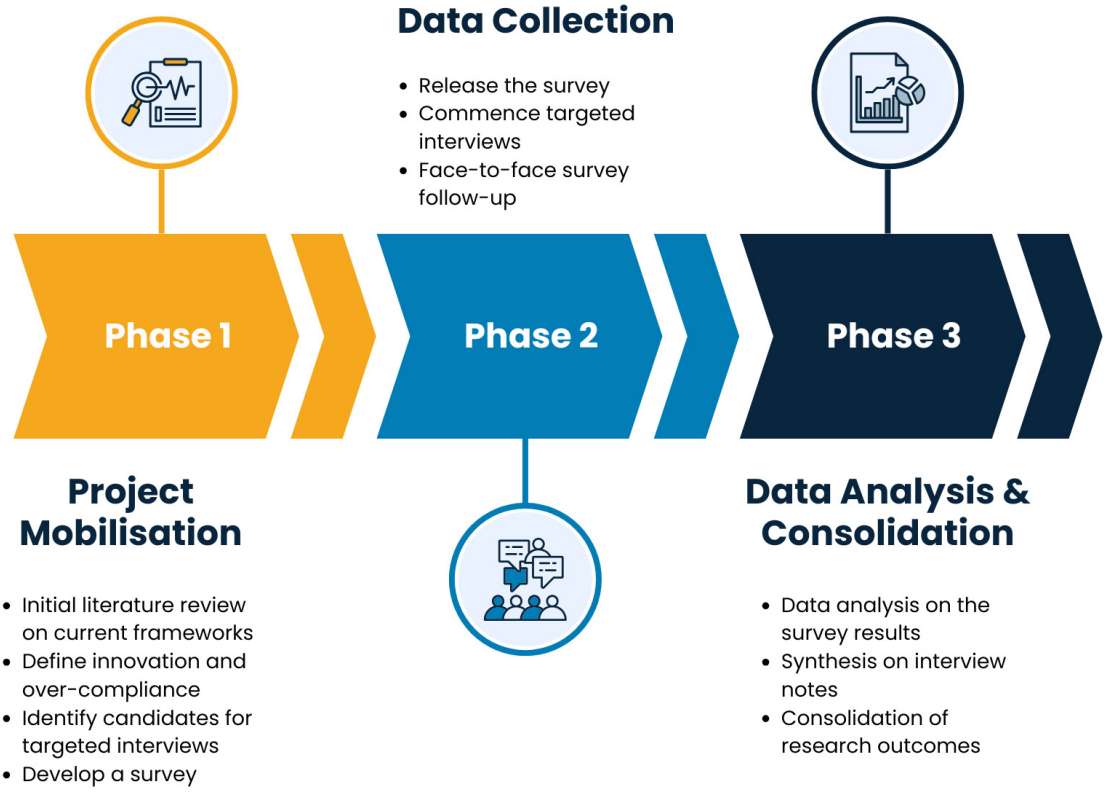


Figure 2 - Project Phases

4.1. Phase 1 - Project Mobilisation

This initial phase was designed to help understand the topic and the existing frameworks for security requirements and procurement processes that SMEs are contractually obligated to comply with. These findings helped define a set of survey questions that would allow participants to contribute their perspectives and experiences on the impact of *over-compliance.*

The survey was written to solicit insights from SMEs but applicable to several sector stakeholders including Primes, regulators and Defence. A mixed-method approach to defining the survey questions was taken, asking contributors for quantitative data to help identify patterns and relationships, and qualitative data to provide deeper insights, to their experiences.

To complement the survey key individuals in industry with known first-hand experience navigating Defence regulation.

4.2. Phase 2 - Data collection

The data collection phase was designed to enable agility in the conduct of follow up interviews with survey participants This agility also provided capacity to pivot scope if other areas of over-compliance were identified and warranted further investigation.

The survey was released on LinkedIn by the authors of this document. Survey responses were reviewed weekly allowing the project team to iteratively evaluate the approach and develop tailored questions for follow-up interviews.

During this phase targeted interviews commenced with representation from SMEs, Primes, regulators and Defence.

4.3. Phase 3 - Data analysis and consolidation

The final phase of research aimed to consolidate findings using both the explanatory and convergent approaches to analysis. The explanatory approach required review and analysis of responses from the survey, and used the qualitative insights gained from face-to-face interviews to detail findings. The convergent approach treated the survey results and interview notes separately, which drove synthesis of common themes to inform the recommendations made in this paper.

5. Findings - SME Survey

SMEs are a critical component of Defence supply chains, yet they face unique challenges in meeting security and compliance obligations designed primarily with larger Primes in mind. While compliance frameworks are essential for national security, less attention has been paid to how their design impacts the innovation capacity of SMEs.

Our survey questions aimed to assess SMEs and their experience with compliance framework in the Defence Industry. The question steered the respondent to explain if there is overcompliance or over regulation in the Defence sector as well as providing recommendations of possible improvements. In summary the results show that SMEs see Defence compliance as important but burdensome, inconsistent, and innovation-limiting. They call for clearer rules, faster approvals, risk-sharing, and more open collaboration to create an environment that enables innovation while maintaining security.

We asked the respondents 10 questions focusing in four major areas: over-compliance, innovation being compromised, procurement and security complexity. The detail of the responses can be found in *Appendix B*. A total of 32 responses were received from different SMEs in the Defence Industry. From the data obtained the following can be summarised:

5.1. Overview of survey results

Most SMEs (24 vs 8) report over-compliance issues affecting innovation.

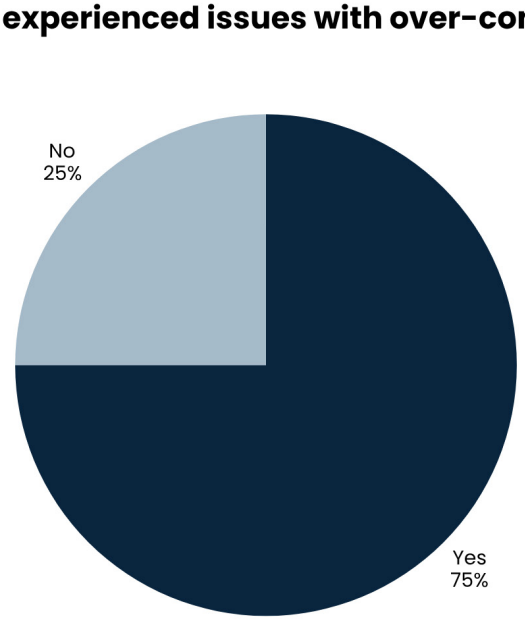


Figure 3 - Responses on issues affecting innovation

Compliance sustainability is inconclusive, with responses split between agreement, disagreement and neutrality

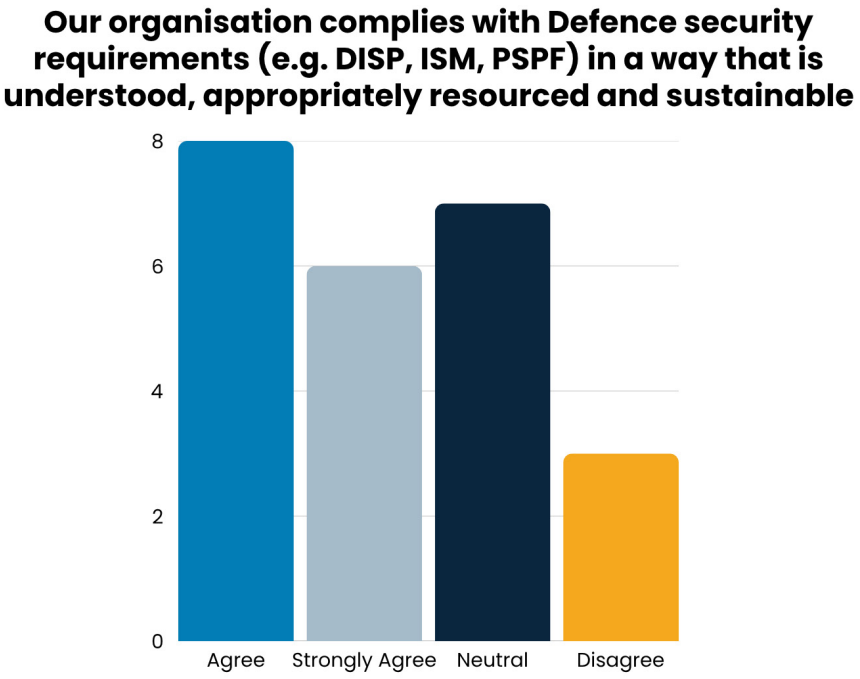


Figure 4 - Compliance sustainability

Innovation abandonment is evenly split (12 yes, 12 no).

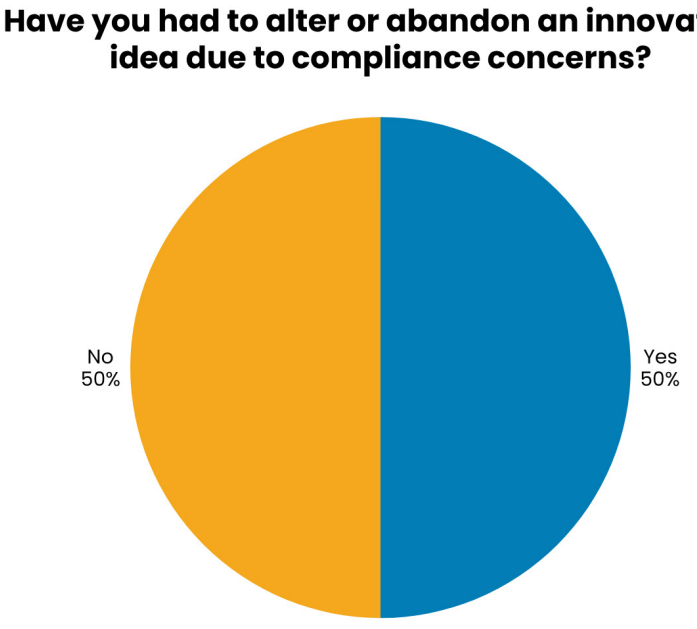


Figure 5 - Abandonment rates

Procurement complexity is widely seen as a barrier to SME engagement.

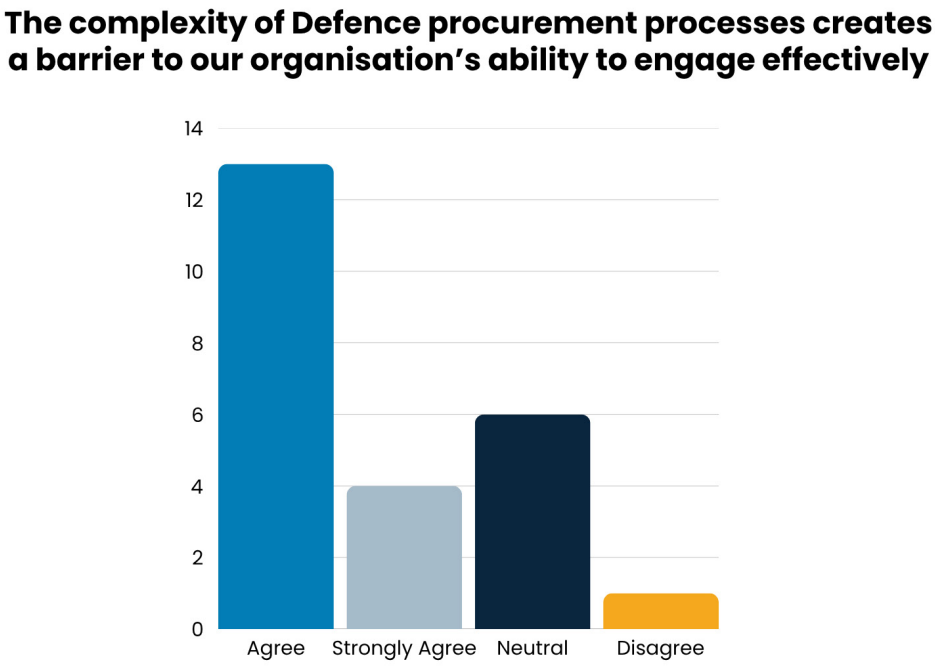


Figure 6 - Complexity as a barrier

5.2. Discussion of survey results

The survey responses reflect a consistent pattern: while compliance with Defence security requirements is acknowledged as necessary, many SMEs perceive it as overly complex, inconsistently applied, and detrimental to Innovation. A deeper look into the "why" reveals three main underlying themes:

1. Ambiguity and inconsistency of standards

Respondents frequently cited overlapping frameworks (DISP, ISM, PSPF, Essential Eight) as burdensome. The "why" lies in the fact that these frameworks are often interpreted differently across contexts, creating uncertainty for SMEs with limited compliance staff. When rules are abstract or inconsistent, SMEs must invest disproportionate effort into interpretation, which consumes resources otherwise available for R&D or product development. This was discussed further in the interview with Emilio de Stefano who agreed that a lot of their clients feel very confused by the requirements from different Primes or CASG.

2. Resource intensity and disproportionate burden on SMEs

A recurring explanation for inhibited innovation is the mismatch between compliance expectations and SME capacity. Unlike Primes with established compliance departments, SMEs operate with finite personnel and financial resources. Respondents describe compliance activities as "costly," "redirecting time and money," and creating "long delays" (e.g. DISP membership, security clearances).

The underlying reason is structural: compliance frameworks are designed with large organisations in mind, yet are applied universally, resulting in SMEs diverting scarce resources away from creative and competitive activities. Based on the responses from the survey, half of the respondents have abandoned submitting solutions due the burden of compliance frameworks and procurement requirements. From the interview with Emilio, it was clear that his company can see that burden reinforced in "business as usual" with most of their clients. He reflected that SMEs employees must wear multiple hats to be able to comply with Defence compliance requirements and in a lot of cases maintaining some of these certifications can become a full-time job. In addition, there is no specific training or guidelines for some of these roles which leaves personnel spending long hours trying to find the right direction.

3. Procurement processes as systemic inhibitors

Beyond technical compliance, the complexity of Defence procurement emerged as a larger barrier. Respondents noted that strict procurement models and flow-down of terms from Primes constrain collaboration and innovation. The "chicken-and-egg" effect appears: SMEs need to meet compliance requirements to collaborate, yet collaboration is needed to justify investment in SMEs. Current procurement frameworks reinforce risk-transfer over collaboration.

Complexity is often mistaken for rigour, constraining SME participation and innovation

5.3. Recommendations from survey respondents

Survey participants were asked for recommendations on how to reduce the burden of over-compliance and create a more SME-friendly ecosystem. Table 2 summarises the recommendations from those participants.

Table 2 - Survey recommendations summary

Theme	Recommendation	Outcome
Scale to risk	Adopt risk-based and proportional DISP/ISM obligations for SMEs.	Enables compliance without overburdening capability.
Simplify frameworks	Rationalise overlaps across DISP, PSPF, ISM, and E8; provide clear mapping tools.	Cuts duplication, builds clarity.
Tailor contracts	Reform ASDEFCON for SME-friendly versions with capped liability, fair IP clauses, and lean templates.	Unlocks fairer participation.
Enable speed	Introduce standard Service Level Agreements (SLA)s for vetting and facility accreditation.	Reduces project slippage and cost.
Support SMEs	Fund compliance assistance programs, e.g. vouchers, templates, or advisory panels.	Improves confidence and reduces attrition.
Promote collaboration	Incentivise co-design, sandbox pilots, and teaming models.	Builds trust and innovation pathways.
Digital coherence	Develop a single Defence Industry portal with once-only data submission.	Increases transparency and efficiency.

6. Findings - Targeted Interviews

6.1. Overview

This section presents consolidated findings from a series of targeted interviews conducted with representatives across Defence Industry. Interviewees included:

- Dr Andy Boud (*Second Wave XR*),
- Mike Hartas (*PMB Defence*),
- AIRCDRE (Ret'd) John Oddie AM CSC (*Aura Group*),
- Graham Priestnall OAM (formerly of Asension, RAN ret' d, and AIDN member)
- John Salerno (*Dedicated Systems*), and
- Emilio De Sefano (*De Stefano & Co*)

Each discussion explored the central research question:

"How does over-regulation and excessive compliance within Defence contracting frameworks impede innovation and participation by Australian industry?"

What emerged was not a shortage of ideas, but a pattern - a repeating cycle that begins with confusion and ends in cost. Participants described a system that responds to every problem with another process, and every delay with another control. Innovation isn't halted by a single barrier; it is slowly buried beneath layers of structure designed to keep Capability Acquisition safe.

These findings are framed through five interlinked friction points between concept and capability - known throughout this project as the *Five C's.*

Together, the *Five C*'s form a culture that energises a self-perpetuating loop:

- Complexity creates confusion.
- Caution emerges, driving adherence to compliance.
- Compliance undermines credibility - good ideas aren't trusted until proven, but can't get proven.
- Credibility compounds cost - in people, cash, and time.
- Cost blowouts justify new controls, re-creating the very complexity that started the cycle.

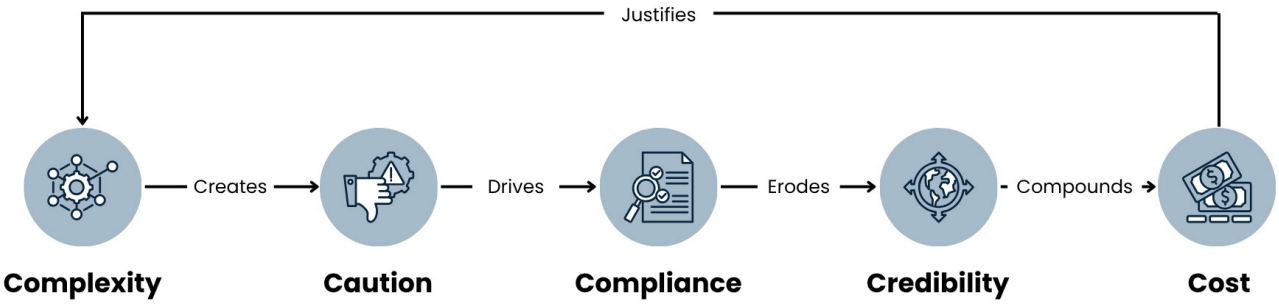


Figure 7 - The Five-C Cycle

This cycle defines the space between concept and capability - where Defence's intent to innovate is consistently overtaken by its instinct to control. The following sections explore each "C" in turn, demonstrating how systemic, behavioural, and cultural forces inadvertently combine to constrain progress and inflate cost. Together, they explain why innovation in Defence often struggles not for lack of talent or technology, but because the system mistakes control for confidence.

6.2. C-1 - Complexity

The cycle begins with complexity. Before caution, compliance, or cost appear, complexity creates confusion - and confusion consumes opportunity. Every interviewee, from Primes to SMEs, pointed to process bloat as the most paralysing feature of Defence procurement. The deeper an organisation sinks into ASDEFCON, the less energy remains for innovation.

Mike Hartas described complexity as the quiet killer of efficiency: "No one person has ever sat down and tried to respond to an ASDEFCON end-to-end." He recounted that in most tenders, the Commonwealth issues the entire suite of documents-security, quality, safety, cyber, environmental-without discrimination. "Defence asks more than most - more than anyone - but doesn't necessarily understand why" he said. They've even been known to mandate innovation - a contradiction in terms that perfectly illustrates how process has replaced purpose. Primes then flow those same clauses downstream, regardless of relevance or scale. "You end up with two choices," Hartas said. "Either you say no because it's impossible, or you sign and pretend you can." For small companies, either path is ruinous. The framework designed to manage complexity instead creates it.

This procedural sprawl extends to oversight. Hartas described Defence's reporting cycles as "managing everything instead of managing by exception." Project teams generate vast amounts of data that nobody analyses. "There's so much reporting that the people meant to make decisions don't have time to read it," he said. The outcome is a paradox:

The more Defence knows, the less it understands.

Graham Priestnall offered a concrete example from the *Defence Innovation Hub* (DIH), where complexity transformed a 12-month transition window into a year of paperwork. "Innovation is risk, but the Hub was run under normal procurement rules," he explained. "We finished Phase Two and should've rolled straight into Phase Three, but commercial stopped it. We lost twelve months re-negotiating risk clauses." For a program meant to accelerate new capability, that delay was terminal. "By the time we got approval, the technology had moved on," Priestnall said. "Innovation can't survive that kind of lag."

Emilio De Stefano observed that this kind of unnecessary complexity extends into the security domain. Because Defence and Primes rarely clarify which accreditation levels are genuinely required, suppliers routinely over-apply for DISP membership "just to be safe." The entire system clogs with paperwork from organisations that never needed certification in the first place.

John Oddie contrasted Australia's labyrinthine like process with what he observed in the United Kingdom, where the Ministry of Defence procured a small fleet of prototype six-wheel-drive electric unmanned vehicles under a brief, outcome-focused contract. He explained that this brevity stood in stark contrast to his experience responding to ASDEFCON-level compliances for relatively projects. He also recalled a domestic case in which Defence's vehicle-fleet acquisition was skewed toward commercially safe choices-Land Cruisers-over technically superior alternatives such as a RAM 3500. "The only measure we didn't meet was turning circle," Oddie said, "and six years later most tradies drive one." His point was not about vehicle type but about mindset: that documentation and conformity often substitute for discernment.

Complexity also breeds inconsistency. Hartas pointed out that within a single ASDEFCON pack, the liability clause may contradict the insurance clause, which contradicts the definition of risk. "At the start it says you're insured for twenty million, halfway through its unlimited liability, and by the end it's both," he said. "If that went to court, no one could explain it." The burden then falls on Industry to interpret contradictions they didn't create.

Even when Defence recognises the problem, simplification efforts are patchy. Initiatives like ASCA show promise but remain constrained by the same institutional reflexes that created DIH's delays. "ASCA was meant to be agile," Priestnall said, "but its early tenders were so broad they got a hundred submissions each. Simpler paperwork doesn't help if the strategy is still unfocused."

The human impact of complexity is fatigue. Innovators spend more time navigating forms than designing solutions. Dr Andy Boud explained that innovation often fails not for lack of evidence but for lack of permission - Defence lacks mechanisms to adopt proven ideas quickly.

Key finding:

Complexity has replaced competence as the marker of rigour. Layers of process, reporting, and review are mistaken for control, but they fragment responsibility and smother initiative. Simplification is not administrative hygiene-it is a strategic necessity. Until Defence accepts that clarity enables confidence, complexity will remain the enemy of capability.

6.3. C-2 - Caution

Where complexity defines the system, caution defines the mindset that sustains it. When cost is high, credibility fragile, complexity rampant, and compliance suffocating, people stop taking risks. Interviewees consistently described Defence as an organisation where the safest decision is no decision at all.

Caution has evolved from prudence into policy.

John Oddie captured the mindset bluntly: "Defence prioritises the comfortable over the beneficial." During his time in uniform and later as an industry leader, he watched the system reward avoidance over initiative. "A bureaucrat's job is to stay a bureaucrat," he said. "Choosing the known supplier guarantees survival; choosing a new idea guarantees attention." The fear of failure is so institutionalised that even mild experimentation can be career-limiting. Public servants, Primes, and SMEs alike learn to navigate by what is least controversial, not necessarily what's most effective.

The consequences are profound. Oddie recounted a titanium sniper-rifle project that Defence neglected to test - despite superior performance - because it was unfamiliar. The decision to buy from a competitor was not technical; it was psychological. "If you pick Barrett and it goes wrong, nobody gets shot," he said speaking figuratively. "Pick the unknown Australian company and it fails, and you're the headline." This risk-averse reflex turns procurement into self-protection.

Graham Priestnall called the behaviour "strategic immaturity." He noted that officials tasked with fostering innovation often lacked the technical literacy to judge it, so they defaulted to delaying or deferring decisions upward. "We end up with five layers of signatures before anyone can say yes," he said. "By the time approval comes, the opportunity's gone." The instinct to escalate rather than act transforms accountability into a negative inertia.

That same dynamic extends into funding authority. Dr Andy Boud described demonstrating a proven virtual-reality training system to Defence. Commanders endorsed it enthusiastically but admitted they lacked the budgetary delegation to adopt it. "They loved it," Boud said. "But they couldn't spend a hundred thousand dollars without Canberra's approval." The result is another paradox: the people closest to the problem are, from Industry's perspective, the least empowered to solve it.

Mike Hartas connected caution directly to misplaced liability. Primes, fearful of bearing contractual risk, push it downstream to SMEs; Defence, fearful of audit exposure, pushes it upstream to Primes. The outcome is a closed loop of fear where every participant manages risk by transferring it to someone else. "Risk should be managed at the appropriate level," Hartas said, "but no one wants to be the one holding it when the music stops."

De Stefano argued that this pattern reflects a deeper mindset issue - an obsession with risk avoidance rather than risk management. “Primes should assume more risk to allow industry to be innovative,” he said. “Managing risk openly beats pretending it doesn’t exist.” His view aligns closely with others who believe Defence’s caution has become somewhat self-defeating.

This environment erodes initiative. Engineers, project officers, and business owners alike learn that doing nothing rarely gets you fired. John Salerno described it wryly: “We were right at the front of the DISP queue, and we slipped because we didn’t have the right mates.” Relationships become risk insurance; capability becomes secondary.

Caution also manifests rhetorically. Defence speeches praise innovation, but the system is built to resist it. “We write Innovation Plans as contract deliverables,” Oddie noted. “It’s performative courage.” The real courage - acting without perfect certainty - remains scarce.

Key finding:

Caution is a major brake on the innovation cycle. It stems not from laziness but from fear - of audit, exposure, and consequence. Until Defence shifts its reward system from avoiding failure to achieving outcomes, the safest path will continue to be the still one. True innovation demands tolerance for error, empowered decision-making, and leadership willing to say yes without waiting for permission. Without that courage, every good idea will remain what the system finds most comfortable: theoretical.

6.4. C-3 - Compliance

That same fear of error finds its comfort in compliance. Interviewees described compliance as the most visible daily burden and the least questioned. It is the habit that feels like accountability but functions as avoidance.

Mike Hartas summarised it best: “Defence limits innovation because it has an overly commercially complex way of trying to do things.” In his view, the system no longer distinguishes between mandatory safeguards and inherited habits. Frameworks such as the Protective Security Policy Framework (PSPF), Defence Security Principles Framework (DSPF), ISM, and *Essential 8* are treated as indivisible wholes rather than adjustable toolsets. “It’s like ordering the entire menu because you don’t know what you’re hungry for,” he said. The result is thousands of pages of duplicated requirements - each theoretically defensible, collectively paralysing.

Nowhere is this more evident than in the pursuit of Defence (DISP) accreditation. John Salerno described a three-year journey marked by waiting, rework, and cost. “Defence paused for six months to reorganise internally,” he recalled. “Nothing moved.” In the meantime, his company had to maintain all the same security measures without the formal certification. “DISP, PSPF and Essential 8 compliance just ends up being a cost for everyone.” When asked how he managed it, Salerno’s answer was blunt: “Earn less profit.” For SMEs, compliance is not a differentiator; it’s an entry fee.

Salerno also noted the irony of Defence mandating frameworks faster than it can process them. Primes are told to subcontract only to DISP-accredited suppliers, but thousands of SMEs remain stuck mid-application. The system's guardians cannot keep pace with its own gatekeeping. As Salerno put it, "They've almost mandated it without considering how fast the mandate would go."

De Stefano's experience shows how this confusion feeds over-compliance. In the absence of consistent messaging, suppliers default to implementing every control available "just to be safe." He also noted that the gaps in formal training or certification pathways for Security Officers leaves individuals guessing at evolving requirements, adding to both stress and error. His recommendation was simple: Defence and Primes must standardise and communicate requirements so that compliance becomes proportionate rather than performative.

Priestnall saw the same pattern inside the Defence Innovation Hub (DIH), where projects intended to accelerate ideas were instead strangled by traditional procurement compliance. His company spent a year renegotiating between phases solely to satisfy contract officers' need for risk documentation. "Innovation is risk," he argued. "but the Hub was run under normal procurement rules. We lost twelve months re-negotiating risk clauses." That paperwork achieved its goal - no one was blamed - but it also achieved nothing else.

Oddie and the team member who interviewed him mused on the irony of some contacts being required to submit an "Innovation Plan" as a contractual deliverable. "You can't force innovation," he said. "If you give someone fifty documents they must comply with, you're actually suffocating it." The intention - to ensure consistent quality - becomes a mechanism for control.

Compliance substitutes curiosity; adherence replaces adaptation.

Even the more agile ASCA model remains vulnerable to the same reflex. Priestnall observed that while proposal templates were shorter, "the underlying procurement rules didn't change." What Defence calls simplification, industry still experiences as supervision by spreadsheet.

Boud's experience with simulation training in Defence highlights the consequence: good ideas simply run out of oxygen. Despite a proven system, the unit lacked discretionary funding to purchase it because policy required everything to route through formal procurement. "They loved it," Boud said, "but there was no mechanism to just say yes."

Key finding:

Compliance has drifted from assurance to avoidance. It protects individuals but not outcomes. The fear of doing the wrong thing has eclipsed the intent to do the right thing. Until Defence distinguishes between necessary governance and habitual bureaucracy, compliance will continue to reward paperwork over performance and will keep innovation exactly where it feels safest - on paper.

6.5. C-4 - Credibility

Beyond systems and procedures lies a subtler constraint - credibility itself. Every interviewee, from ex-service senior leaders to SME executives, described an entrenched scepticism toward new entrants and unconventional ideas. It is a quiet hierarchy of trust in which who you are outweighs what you offer. In Defence, credibility is currency-and its exchange rate heavily favours the familiar.

Air Commodore (Ret'd) John Oddie captured this succinctly: "Defence prioritises the comfortable over the beneficial." He explained that choosing a known multinational is a "safe" decision; if the project fails, the blame lands softly. Selecting a small Australian firm, however, exposes a public servant to personal scrutiny. "People need to be a bit brave," he said. "It's not a courageous decision to go with the comfortable option." This fear of reputational risk drives a preference for incumbency that rewards pedigree over performance.

The pattern mirrors *Tall Poppy Syndrome* - the tendency to cut down those who stand out.

Innovators who challenge doctrine or offer disruptive capability are often dismissed as unrealistic or immature. Oddie recalled designing a 3D-printed titanium rifle that was lighter and more accurate than its imported equivalent. Despite demonstrable success, Defence never test-fired it. They went with another supplier because that supplier was a known quantity. "If you've got a new idea, they'll pat you on the head and buy the one they already trust," he remarked. "It's comfortable."

Mike Hartas observed the same instinct within procurement culture: "There's a desire to push risk down rather than manage it. We treat every SME like a liability until proven otherwise." In his view, credibility becomes a defensive mechanism-a justification for rigid contracting rather than a measure of competence. This over-caution undermines the very trust networks required for innovation to flourish.

Priestnall, extended the argument to Defence's internal environment, describing "educational and cultural immaturity" among officials tasked with assessing technical proposals. Without the background to recognise potential, decision-makers default to commercial comfort zones. "By focusing so much on preventing risk, they actually increase it," he said. The safe choice consumes more money and time, delivering less capability.

The issue also manifests in resourcing authority. Boud recounted demonstrating a battle-training system that significantly improved learning outcomes. The Commander he demonstrated it to called it "fantastic" but lacked discretionary funding to adopt it. Innovation died not for lack of evidence, but for lack of permission. "It's not that they don't believe in it," Boud said. "They just can't act on it." When credibility is bureaucratised, judgment loses value.

Salerno offered a counterpoint that reinforced the same theme: credibility can be gained-but only by mirroring the behaviour of Primes. SMEs that over-invest in compliance are eventually accepted, not because their ideas improved, but because they learned to look familiar. "Once you tick all the boxes, they'll talk to you," he said. "Until then, you're just noise."

Key finding:

Credibility has become the gatekeeper of innovation. Defence's aversion to reputational risk privileges established brands and diminishes local ingenuity. The Tall Poppy instinct ensures that the safest ideas are heard first and the boldest last. Until credibility is earned through capability rather than comfort, Australia's most inventive minds will keep waiting for permission to contribute.

6.6. C-5 - Cost

The cumulative effect of these behaviours is measured in cost - not just financial. As John Oddie later reflected, beyond dollars, time, and people lies "the cost of lost opportunity - the innovation that never happens because Defence sails past it on a sea of paperwork While Defence policy often frames regulation as a safeguard against financial risk, those at the delivery end experience it as the opposite - a multiplier of cost, delay, and duplication. Every layer of compliance represents another hand in the pocket of innovation.

Hartas was unequivocal. He argued that the financial burden of Defence contracting begins the moment the Commonwealth issues an ASDEFCON pack.

"The over-regulation starts from the contract," he said. "No one sits down and works out what's needed. The whole suite of documents is dumped on the table, and then everyone starts reporting monthly on everything whether it matters or not."

The result is hundreds of thousands of dollars in staff hours spent on progress reports that add no value to capability.

This cost pressure cascades down the supply chain. Hartas described the flow-down of commercial terms as one of the most damaging practices in the Australian system. Primes routinely pass clauses written for billion-dollar programs - including unlimited liability - to SMEs turning over only a few million a year.

"If you flow unlimited liability to a supplier worth twenty million a year, you've already made the contract unworkable," he noted. Companies either walk away or sign something they cannot realistically comply with, absorbing the risk to maintain relationships. In both cases, innovation suffers: the capable but cautious SME withdraws, while the desperate one overextends and risks everything.

Priestnall highlighted how the same dynamic drains taxpayer value. His team delivered an electronic-warfare satellite demonstrator under the Defence Innovation Hub, at a cost of roughly eight million dollars. When the program folded, no follow-on project existed to adopt the technology.

"Eight million bucks got spent, and it's sitting on a shelf," he said. "We generated sovereign capability, trained thirty-seven engineers, and still lost the lot because nobody budgeted to transition it." In Priestnall's view, the Commonwealths earlier approaches fund innovation as a project, not as a pathway - so the return on investment ends at milestone delivery.

For smaller firms, compliance costs are existential. Salerno of explained that his company's pursuit of DISP membership required new governance frameworks, cybersecurity upgrades, and external consultants, all before seeing a cent of new business. "DISP, PSPF and Essential 8 compliance just ends up being a cost for everyone," he said. These costs cannot be recovered under existing panel rates, effectively reducing profit margins across the sector. "If you were a new company without a customer base, this would hurt quite a bit."

De Stefano reinforced this, noting that costs are magnified by uncertainty. Many SMEs over-invest in cyber tools and governance roles simply to appear compliant. "Establishing and maintaining Essential 8 controls is expensive enough," he said, "but it's worse when no one tells you what level you actually need." Without clear direction, firms appoint security officers, buy duplicate systems, and pay for external consultants-an expensive insurance policy against ambiguity.

The collective sentiment is that money spent on regulation rarely buys assurance - it buys friction. Instead of incentivising prudent risk management, Defence's contracting approach compels over-insurance, redundant oversight, and parallel reporting chains that expand the bill while shrinking the output. Participants were unanimous that Defence pays twice for every innovation: once to demand compliance and again to repair the damage that compliance causes.

Key finding:

Regulation intended to protect public funds has created an economy of paperwork. The true cost of capability is not the prototype on the bench, but the bureaucracy surrounding it. Until cost accountability shifts from process to outcome, innovation will remain the first casualty of over-regulation.

6.7. Five-Cs - Conclusion

Across all Five C's a consistent narrative emerges:

Defence is not short on ideas; it is short on freedom to act on them.

The ecosystem between concept and capability has become defined by protection rather than progression. Each control mechanism, once created to ensure accountability, now competes against innovation itself.

What these interviews reveal is not failure, but fatigue. Industry continues to show ingenuity, but that energy is absorbed by the machinery of assurance - too costly to sustain, too cautious to reform from within. As one interviewee put it, "Innovation is treated like a risk event, not an opportunity."

The path forward, therefore, is not another framework or funding line. It is a recalibration of trust, authority, and tolerance for imperfection - a system that manages risk through understanding, not avoidance. The following section presents recommendations drawn from these insights, aimed at rebalancing oversight with empowerment and transforming the Five C's from barriers into enablers of capability.

7. Discussion

7.1. The Devil's Advocate: Is Defence Really the Problem?

At first glance, it is tempting to conclude that Defence's culture and frameworks are the primary barriers to innovation. Yet, playing devil's advocate, it is worth asking whether industry's frustrations arise not only from over-regulation, but from a mismatch of expectations.

Defence's mandate is assurance - to protect life, secrets, and taxpayer value - whereas industry's mandate is agility and competition. When these imperatives collide, "friction" may be unavoidable rather than pathological. From this angle, the 5 C's are not solely symptoms of dysfunction but artefacts of a system optimised for risk control rather than experimentation. Defence does not set out to stifle innovation; it sets out to guarantee reliability. The issue is that the mechanisms designed for control are now being applied universally, even when the consequence of failure is negligible.

This counter-position reframes the debate: perhaps Defence's problem is not too much compliance, but too little differentiation. A missile and a maintenance app are treated with equal caution. A truly "smart" system would scale governance to risk, not apply governance as risk avoidance. The challenge, then, is not to abolish compliance but to make it intelligent - to allow innovation to coexist with accountability.

7.2. Security: Compliance is Both a Shield and Shackle

The security frameworks examined - DISP, PSPF, ISM, and the Essential Eight - exist to protect national secrets and critical infrastructure. Interviewees and survey respondents alike acknowledged that without these guardrails, Defence's trust in industry would erode. From this viewpoint, compliance is the price of entry into a sensitive ecosystem and an enabler of confidence between Defence and suppliers.

However, our data show that these same controls can evolve into shackles. When requirements are ambiguous, duplicated, or applied indiscriminately, they consume the very resources that could otherwise fund secure-by-design Innovation. SMEs implement full DISP membership "just to be safe," hire qualified but inexperienced security officers, and maintain parallel systems to meet overlapping frameworks.

The result is a paradox: Defence's security posture intends to harden the enterprise but instead disperses capability into administration. Security, in its current form, has become less about protecting secrets and more about protecting reputations.

The opportunity lies in proportionality. A tiered, risk-based model - where compliance obligations scale with the sensitivity of work - could preserve assurance while returning oxygen to innovation. In essence, Defence must move from a “compliance-as-policy” culture to a “security-as-outcome” mindset.

7.3. Procurement: Efficiency, Accessibility, and Fairness

Procurement emerged as both the linchpin and bottleneck of innovation. The ASDEFCON suite, while built to ensure fairness and probity, now functions as a deterrent to participation. SMEs perceive the process as costly, opaque, and dominated by incumbents. Interviewees described tender packs thousands of pages long, contradictory clauses, and year-long approval cycles - a level of procedural depth more suited to billion-dollar programs than small, experimental projects.

From a procurement-policy standpoint, these measures uphold equality before the contract - no firm receives special treatment. Yet equality is not the same as equity. Treating a ten-person SME and a multinational Prime under identical compliance regimes achieves procedural fairness but practical exclusion. The administrative load alone can disqualify newcomers from even bidding, consolidating market power in the hands of a few.

Conversely, initiatives like ASCA and the Defence Innovation Hub illustrate Defence’s intent to reform. Their shortfalls stem not from malice but from inertia: simplification of templates without simplification of behaviours. True efficiency will come when procurement shifts from control-centric to outcome-centric-valuing demonstrable capability over perfect paperwork, and designing contracting pathways that match project scale and risk.

7.4. Trade-offs: Innovation vs Assurance

Defence’s greatest paradox is that the same structures that ensure reliability can also immobilise progress. Innovation demands iteration, but assurance demands certainty. The two are not mutually exclusive, yet the current system treats them as opposites.

Every clause, clearance, and review seeks to prevent the next headline failure - a rational instinct in a high-stakes environment - but each also delays the next breakthrough. The interviews repeatedly returned to this tension: Innovation is risk, but the system tries to eliminate it through paperwork.

Balancing these imperatives requires cultural and structural maturity. Assurance should evolve from an end-state to a continuum - an ongoing calibration between experimentation and evidence. This might mean tolerating controlled failure within bounded environments (for example, sandbox trials or limited-scope contracts) rather than demanding perfection before adoption.

Risk management, not risk avoidance, is the discipline that reconciles innovation and assurance. In short, innovation and assurance need not be opposing forces - they can coexist when Defence learns to scale oversight to consequence.

8. Recommendations

Across the survey, interviews, and case studies, one conclusion is clear: over-compliance is not a single actor's fault but a system's reflex. Defence's frameworks were built to prevent catastrophe, not to enable creativity, and yet the same discipline that protects capability can also suffocate it when applied without proportion.

SMEs are caught between two imperatives - to comply and to compete.

Defence is caught between two fears - losing control and losing credibility.

Reconciling these tensions demands not deregulation but differentiation: clarity on when to be strict, when to be swift, and when to be brave. Only then can the Five C's - Complexity, Caution, Compliance, Credibility, and Cost - transform from constraints into catalysts for sovereign capability.

To rebalance the system, Defence must pursue proportionality (rigour scaled to risk) and differentiation (multiple pathways suited to innovation maturity). The following recommendations propose practical steps to achieve that balance.

8.1. Recommendation 1 - Refine and Expand Innovation Pathways

1A - ASCA: Defining Requirements, Not Products

Major General Hugh Meggitt, Head of ASCA, has famously cautioned industry that "If I ask for an iron, don't sell me a toaster."

The intent is sound - to ensure Defence receives solutions aligned with the National Defence Strategy and the needs of the ADF - it also reveals the danger of asking for an appliance instead of an outcome. Innovation more often comes from repurposing rather than invention.

With a bit of innovation - and the odd scorch mark in testing - you could probably use the toaster to iron a shirt, or, using proper engineering lexicon: to remove a crease from a specified fabric. That's what happens when you describe the problem by outcome instead of appliance.

This kind of requirements-driven specification empowers industry to propose creative, perhaps unconventional technologies that still deliver the effect Defence seeks.

It maintains Defence's assurance framework while allowing lower-TRL innovations to compete on merit rather than conformity. ASCA should therefore adopt a requirements-driven specification model, providing measurable outcomes while remaining technology-agnostic.

Defence doesn't need more irons, it needs to empower courage in people to look at the toaster and ask "What else could this do?"

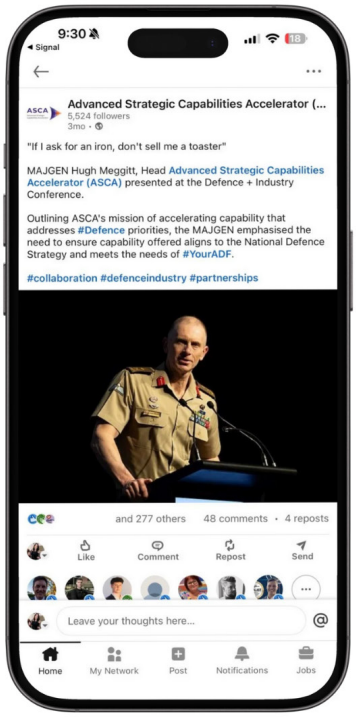


Figure 8 - MAJGEN Hugh Meggitt Addresses the Defence & Industry Conference (LinkedIn)

1B - ASCA Pathway 2 - A Gateway for Unsolicited High-TRL Innovations

In his remarks, MAJGEN Meggitt also emphasised that capability offered must align to the National Defence Strategy and the needs of the ADF.

We recognise and support that imperative; however, a purely "ask-and-answer" model risks excluding innovations that Defence has not yet imagined it needs.

To complement the requirements-based stream, ASCA should establish a second channel for unsolicited, high-TRL innovations.

This would allow Australian industry - including the metaphorical "toaster makers" - to present mature technologies that could be adapted to Defence purposes, even those that ultimately "shall remove a crease" through unexpected means.

Such a dual-pathway approach would:

- Encourage continuous engagement between Defence and innovators, not just during formal proposal rounds;
- Enable faster field trials and end-user feedback to test operational relevance; and
- Increase visibility of emerging technologies that align indirectly with Defence outcomes but fall outside current tenders.

Defence already performs well in experimentation, but true innovation requires structured adoption.

By formalising a second, strategically aligned innovation channel, ASCA can transform experiments into capabilities while maintaining coherence with national priorities.

As ASCA evolves, further investigation should be undertaken into how effectively its outputs translate into capability at the user level - ensuring that innovation pipelines deliver tangible benefit to the ADF, not just process efficiency within Defence.

8.2. Recommendation 2 - Re-calibration of Defences Risk Appetite

Defence's culture of caution - rooted in legitimate accountability - has evolved into risk avoidance. To enable innovation, the Department must shift toward risk management matched to consequence, where rigour follows risk rather than risk driving rigour.

This cultural transformation will not be easy across a workforce of more than 100,000, but several targeted levers can accelerate it:

- Embed proportional assurance principles in policy and contracting guidance so that minor projects and prototypes are not subject to the same scrutiny as major capital acquisitions.
- Decentralise decision-making authority to allow program managers to approve low-risk trials without Canberra-level sign-off.
- Revisit Australian Industry Capability (AIC) frameworks to ensure smaller contracts are reserved for direct engagement with SMEs rather than being subsumed under Prime contractors.
- Reward informed risk-taking in performance frameworks-celebrating lessons learned from controlled failure rather than punishing imperfection.

The objective is not to make Defence reckless, but to make it responsive: managing risk through understanding, not through avoidance.

8.3. Recommendation 3 - Simplification and Clarification of Pathways

Despite the creation of the *Office of Defence Industry Support* (ODIS) to help SMEs navigate Defence, industry feedback indicates that it remains fragmented and difficult to use.

Firms frequently report uncertainty about where to begin, which frameworks apply, and how to interpret overlapping requirements for security, cyber, and procurement.

Defence should therefore invest in a single, authoritative "*Defence-Ready*" portal that consolidates essential information into concise, actionable guidance:

- A one-page compliance map outlining baseline obligations for security, cyber, export control, and procurement.
- Interactive checklists and templates tailored to business size and contract risk level.
- Clear escalation pathways to human advisors within ODIS or Defence for complex cases.

The goal is clarity, not more policy. By reducing ambiguity, Defence can lower the barrier to entry for innovative SMEs and free both sides from unnecessary administrative friction.

- Practical framework for SMEs to navigate compliance while pursuing innovation.
- Possible recommendations for Defence/government to balance compliance and innovation.
- Actionable steps for industry stakeholders

9. Conclusion

In the end, the challenge for Defence and industry is not one of imagination but of permission.

Australia's Defence ecosystem holds the talent, technology, and ambition to deliver world-class capability, yet its energy is too often absorbed by the machinery of assurance.

Implementing these recommendations would begin to reverse that balance - shifting compliance from a reflex of control to a framework of confidence.

When governance scales to consequence, when risk is managed rather than feared, and when requirements describe outcomes instead of products, innovation can thrive within the very systems built to protect it.

The path forward is therefore one of proportion, transparency, and trust: a Defence enterprise where creativity is not a deviation from process but a demonstration of it - and where Australian ideas are given the clarity and courage to become Australian capability.

10. References

- Abernathy, W.J. & Utterback, J.M., 1978. Patterns of industrial Innovation. Technology Review, 80(7), pp.40-47.
- Ashford, N.A. & Hall, R.P., 2011. Technology, Globalization, and Sustainable Development: Transforming the Industrial State. New Haven: Yale University Press.
- Baldwin, R., Cave, M. & Lodge, M., 2012. Understanding Regulation: Theory, Strategy, and Practice. 2nd ed. Oxford: Oxford University Press.
- Blind, K., 2012. The influence of regulations on Innovation: A quantitative assessment for OECD countries. Research Policy, 41(2), pp.391-400.
- Christensen, C.M., 1997. The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail. Boston: Harvard Business School Press.
- Coglianese, C., 2012. Measuring regulatory performance: Evaluating the impact of regulation and regulatory policy. OECD Expert Paper No. 1. Paris: OECD.
- Department of Defence 2023, Establishment of the Advanced Strategic Capabilities Accelerator (ASCA), Commonwealth of Australia, Canberra, viewed 14 November 2025, https://www.defence.gov.au/about/strategy/advanced-strategic-capabilities-accelerator
- Department of Defence 2024, Defence Industry Development Strategy, Commonwealth of Australia, Canberra, viewed 14 November 2025, https://www.defence.gov.au/about/strategy/defence-industry-development-strategy
- Dodgson, M., Gann, D. & Phillips, N., 2011. The Oxford Handbook of Innovation Management. Oxford: Oxford University Press.
- Gans, J.S. & Stern, S., 2003. The product market and the market for "ideas": Commercialization strategies for technology entrepreneurs. Research Policy, 32(2), pp.333-350.
- GAO (U.S. Government Accountability Office), 2020. Defense Acquisitions: DOD's Use of Other Transactions for Prototype Projects Has Increased. GAO-20-84. Washington, DC: GAO.
- Gunningham, N. & Grabosky, P., 1998. Smart Regulation: Designing Environmental Policy. Oxford: Clarendon Press.
- OECD, 2018. Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation. 4th ed. Paris: OECD Publishing.
- Schumpeter, J.A., 1934. The Theory of Economic Development. Cambridge, MA: Harvard University Press.
- Tushman, M.L. & O'Reilly, C.A., 1996. Ambidextrous organizations: Managing evolutionary and revolutionary change. California Management Review, 38(4), pp.8-30.
- US Department of Defense 2025a, Transforming the defense acquisition system into the warfighting acquisition system to accelerate fielding of urgently needed capabilities to our warriors, memorandum, Washington DC, viewed 14 November 2025, https://media.defense.gov/2025/Nov/10/2003819439/-1/-1/1/transforming-the-defense-acquisition-system-into-the-warfighting-acquisition-system-to-accelerate-fielding-of-urgently-needed-capabilities-to-our-warriors.pdf

- US Department of Defense 2025b, Reforming the joint requirements process to accelerate fielding of warfighting capabilities, memorandum, Washington DC, viewed 14 November 2025, https://media.defense.gov/2025/Nov/10/2003819442/-1/-1/1/reforming-the-joint-requirements-process-to-accelerate-fielding-of-warfighting-capabilities.pdf
- .US Department of Defense 2025c, Unifying the department's arms transfer and security cooperation enterprise to improve efficiency and enable burden-sharing, memorandum, Washington DC, viewed 14 November 2025, https://media.defense.gov/2025/Nov/10/2003819440/-1/-1/1/unifying-the-departments-arms-transfer-and-security-cooperation-enterprise-to-improve-efficiency-and-enable-burden-sharing.pdf
- Utterback, J.M., 1994. Mastering the Dynamics of Innovation. Boston: Harvard Business School Press.

11. Appendix A - Acronym List

Acronym List

Acronym	Expanded	Definition
ADF	Australian Defence Force	Australia's military; the ultimate end user of Defence capability and Innovation discussed in the report.
AIC	Australian Industry Capability	Policy framework intended to increase Australian industry participation in Defence projects.
AIDN	Australian Industry & Defence Network	Industry association representing Defence SMEs, referenced in relation to interviewees' backgrounds.
AM	Member of the Order of Australia	Australian national honour; appears in post-nominals for an interviewee.
ASC	ASC Pty Ltd	Australian naval shipbuilding and sustainment company; part of the stakeholder list.
ASCA	Advanced Strategic Capabilities Accelerator	Defence organisation established to accelerate Defence Innovation; central to Recommendation 1.
ASDEFCON	Australian Standard for Defence Contracting	Suite of standard Defence contract templates and conditions; repeatedly cited as a source of procurement complexity.
CASG	Capability Acquisition and Sustainment Group	Group within the Australian Department of Defence responsible for acquiring and sustaining capability; referenced in interview material.
CSC	Conspicuous Service Cross	Australian Defence honour; appears in post-nominals for an interviewee.
DIH	Defence Innovation Hub	Former Defence program to fund and mature innovative Defence capability proposals; discussed in the interviews as a case study.
DILP	Defence Industry Leadership Program	Leadership program delivered by the Defence Teaming Centre and Skills Lab; the context for the project team.

Acronym	Expanded	Definition
DISP	Defence Industry Security Program	Defence security accreditation program for industry; a key security framework examined in the report.
DTC	Defence Teaming Centre	South Australian Defence industry association; co-hosts the DILP and is thanked in the acknowledgements.
DSPF	Defence Security Principles Framework	Internal Defence framework that sets security principles; cited as part of the wider security compliance environment.
E8	Essential Eight	Australian Cyber Security Centre's eight recommended mitigation strategies; part of the cyber compliance burden on SMEs.
FAR	Federal Acquisition Regulation	Primary set of rules governing United States federal procurement; referenced in international comparisons.
GAO	Government Accountability Office (United States)	US oversight body reporting on Defence acquisition approaches, including OTAs, in the references.
IDF	Israeli Defence Force	Israel's military; used as an international example of rapid, iterative Defence Innovation.
ISM	Information Security Manual	Australian Government Information Security Manual; sets baseline cyber security controls relevant to Defence suppliers.
ISO	International Organization for Standardization	Developer of international standards such as ISO 44001; referenced in relation to collaboration standards.
MVP	Minimum Viable Product	Basic, early version of a product used to test and learn quickly; contrasts with risk-averse approaches in Defence.
OAM	Medal of the Order of Australia	Australian national honour; appears in interviewee post-nominals.
ODIS	Office of Defence Industry Support	Defence office intended to help industry navigate Defence entry and requirements; proposed for strengthening in Recommendation 3.

Acronym	Expanded	Definition
OECD	Organisation for Economic Co-operation and Development	International organisation cited in reference material on Innovation measurement and policy.
OTA / OTAs	Other Transaction Authority / Other Transactions	Flexible US Defence contracting mechanism outside the standard FAR; used to engage non-traditional suppliers.
PSPF	Protective Security Policy Framework	Australian Government protective security framework; forms part of the layered security requirements applied to SMEs.
R&D	Research and Development	Systematic work to create or improve products, services, or processes; central to discussions of Innovation capacity.
RAN	Royal Australian Navy	Australia's naval service; appears in the background of one of the interviewees.
SLA	Service Level Agreement	Agreed performance standard or turnaround time; suggested for use in accelerating vetting and accreditation processes.
SME / SMEs	Small and Medium Enterprise(s)	Smaller businesses that form a critical part of the Defence supply chain and are the primary focus of the research.
TRL / TRLs	Technology Readiness Level(s)	Scale used to measure the maturity of a technology; used when discussing Innovation pathways and unsolicited proposals.
UK	United Kingdom	Country used in international comparisons of Defence procurement and Innovation practices.
US	United States	Country referenced in relation to FAR, OTAs, and GAO reports on Defence acquisition.
VR	Virtual Reality	Immersive simulation technology; appears in interview examples of Innovation in training systems.

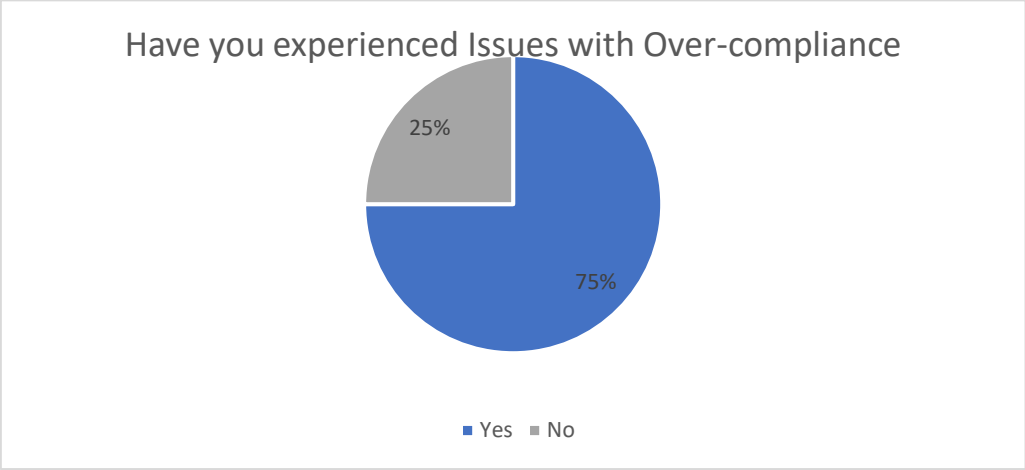
12.Appendix B – Survey Data

Appendix B- Survey Results

Question 1:

In your experience in Defence Industry, has your Small to Medium Enterprise experienced issues with over-compliance to regulations that have impacted creativity and innovation?

Yes	No
24	8

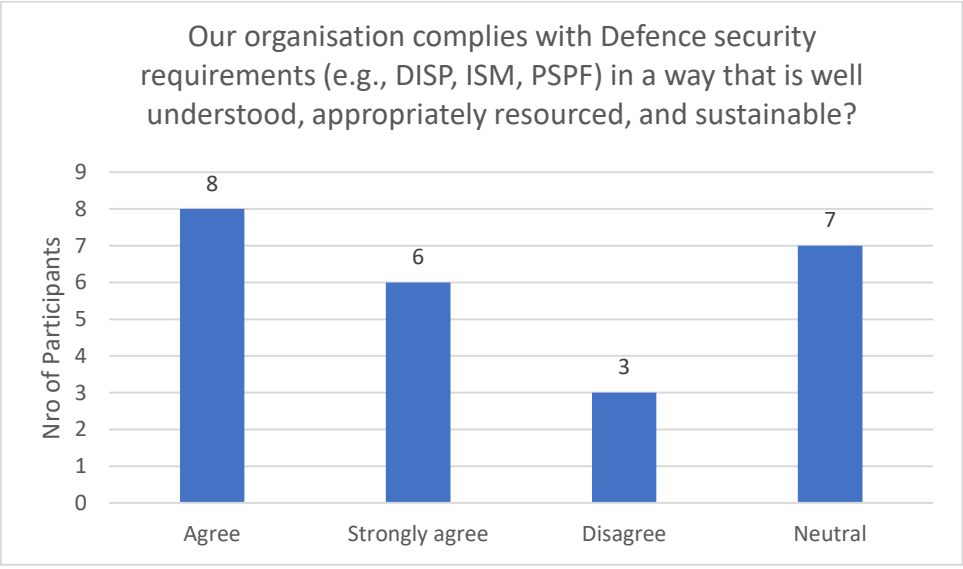


Note: Respondents who Replaceed no to this question skipped directly to question 20. The remaining questions therefore only have 24 responses.

Question 2:

Our organisation complies with Defence security requirements (e.g., DISP, ISM, PSPF) in a way that is well understood, appropriately resourced, and sustainable.

Strongly Agree	Agree	Neutral	Disagree
6	8	7	3



Question 3:

Optional: Please comment on any challenges you've faced in meeting these requirements

ID	Replace
3	DISP, ISM, DSPF and DSPF differ in the way they are written making it difficult to comply with 1 let alone them all.
5	The key challenge is that a small start-up business only has enough money to become operationally viable and to stay alive maybe until first contract. While pursuing compliance to defence standards was something I have seen a lot of, actually funding demonstrated compliance and assigning scarce human resources to such compliance can quickly kill a company in its earliest phases. We have always taken a view that you get us on contract with enough margin we can then fund and resource demonstrated compliance, until then Defence is too hard to engage.
6	There was often different interpretation from different entities on the rules or compliance. Most frustrating was frequently the inability to discuss to explain why we approached an aspect in a particular way and which we believed complied to the required out come.
7	The ISM and PSPF are sufficiently abstract, and in some instances, contradictory, that even government security personnel are often unable to provide any clarity or guidance on how to comply
8	Long delays for processing DISP membership. E8 ML2 compliance for entry level DISP Cyber is expensive for small business. And it is only for DISP related communication. Any project related information (Official Sensitive) requires a separate IT certification (DIACB) which can take years.
10	Processing delays with both DISP and individual security clearances
11	I find the requirements for DISP and the domains to be fairly disjointed. Numerous times I've been told that "There is more information on the DPN". Great, except if I'm applying as a organisation who has never worked with Defence or I do not have access to the DPN, then I can't SEE that additional information.
13	Main challenges are to do with the constant changes. there is significant issues where the current requirements such as DISP are ok for day to day business, such as using Office suite of products, but you cannot develop software in a DISP accredited environmet, and you shouldn't do defence work on non accreditated networks, so the level of compliance required stiffles the ability to develop new systems for defence.
14	Defence staff not being aware of, or familiar with, Defence's regulatory requirements.
15	With the 30 September 2024 update to the DSPF now stipulating the requirement for all DISP members to be compliant to Essential 8 ML2 on their corporate network communicating with Defence, this presents significant additional cost implications to SMEs. As a security business ourselves, we understand the requirements well, however for our clients who we help to attain and maintain DISP there have been significant challenges for them in understanding and implementing particularly the ICT requirements, as well as significant investments to become compliant and maintain it.
17	The move to full E8 has increased costs. The lack of a collaborative cloud based environment means the cost of having ICT meet CoA needs is significant.
19	Some DISP requirements around IT security are overly restrictive based on the level of risk to the organisation and Defence, especially at the entry level IT security

ID	Replace
23	One of the challenges is time. Creating processes and adhering to them is expensive and time consuming, and takes a lot of effort. The technical solutions are not a large challenge for us, it is more establishing the internal business processes.
25	Financial given we're a small business, but it's important to us so we proactively stage our investments in ensuring compliance and continuous improvement.
27	Recent changes have become more onerous and poorly communicated. As an SME, we do not have the revenue to support a full time USO, and as such, this is a secondary duty for a number of staff.
28	Time and effort to get security in place, greatly impacts time to innovate and engage with Defence.
29	Cost to attain and sustain DISP

Question 4:

What security compliance requirements (if any) do you find particularly burdensome or unclear?

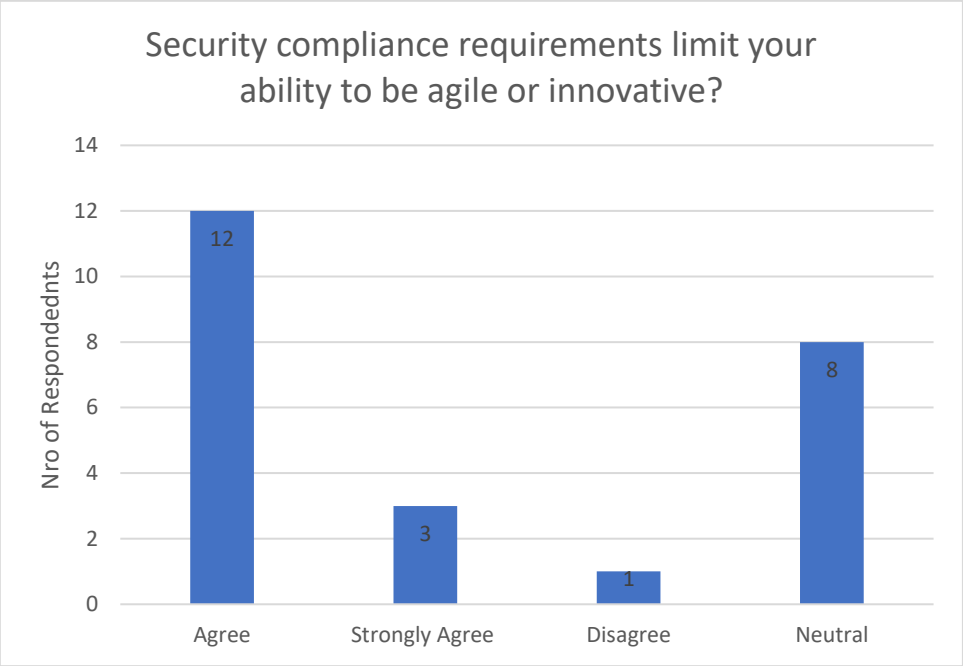
ID	Replace
1	E8
2	Many areas are open to interpretation so mitigating the risk of inadvertently breaching takes significant effort.
3	General requirements
6	Our parent company was working to a NIST standard to comply with American requirements, but was also working towards the ISO standard. At the time neither were recognised as compatible to DISP. Our DISP audit was outsourced to a third party which made it more complicated to achieve the audit. We finally had to engage with a third party ourselves to argue the nuances of the requirements. Altogether it cost both time and money.
7	Data controls, particularly on data transfer mechanisms, that are often beyond impracticable, but actually preclude effective outcomes, even when an analysis of the method demonstrates no risk. And use of security assured PEDs in elevated security zones
8	Cyber security compliance is overly complex for Official Sensitive DISP-related information.
10	DISP pillars around essential 8
11	Cybersecurity guidance again feels disjointed and unorganised. Essential 8 is a solid framework. But the effort required and support provided (e.g. uplift grants) was rather lacking I found. Not to mention that Essential 8 is written as a Windows framework with sometimes vague goals/guidelines. Guidance around ITAR is almost non-existent and I feel is one of the most misunderstood requirements in Defence Industry. You can consult the ITAR framework directly, but it is a US regulation written for US context (e.g. 'only US personnel may...'). Some specific guidance with how it applies to Australian Defence Industry would be invaluable.
13	Typically the most challenging is trying to remain compliant in a changing landscape. Particularly when changes are made during a contract, and have additional costs associated with them, that were not captured in the original budget.

ID	Replace
14	Overseas travel.
15	Essential 8 Maturity Level 2 (for DISP) - cost implications mainly for SMEs. CMMC / NIST 800-171 - lack of clarity around when/where it will apply. Interplay between the two above standards - there are similarities between the two, however what is lacking is a clear indication of where they may be required together within supply chains within Australia. Additional security requirements for nuclear supply chains - awaiting further clarity. Security Clearance reciprocation/recognition across AUS / UK / US - work being done, still not 100% clear. Export Controls (ITAR, FMS, EAR) - complex area that impacts quite a few SMEs who may not have budget to dedicate resources to understanding and managing it. It is also common for the ultimate buyers to be unclear about the requirements they need to pass through to their supply chains, primarily around the enforcement of DISP and at what levels.
17	Difficult to manage security clearances without a sponsor
19	ASD E8 Level 2. for Entry level DISP
21	DISP assessors have a subjective view of each application.
22	For non-security companies, there is a lot of compliance and documentation to get their heads around.
23	The US CMMC standard does not provide clear guidance on the appropriate implementations of certain policy artefacts. Particularly around the appropriate levels of documentation for System Security Plans. Advice and guidance around secure product development and software security standards is a specialist and niche skill and process, and it can be difficult to understand the requirements. For smaller businesses - the security uplift required for implementation of certain security technologies can be burdensome.
25	Data sovereignty requirements where for a long time these requirements were very grey and not well documented. Also, any security requirements relating to AUKUS are still unclear and seem to differ depending on who you're talking to (e.g. which Prime). In some cases, the advice coming from these Primes is down right wrong and misleading, potentially reducing the number of Australian companies that can partake in these projects or at a minimum, costing them hundreds of thousands of dollars in investment where the need is not legitimate.
26	DISP
27	Not in order of priority however, recent assertion that ALL overseas travel is a trigger for a member to submit a Change in Circumstances. This is a very recent addition to the PSPF Controls, that was not advertised at all. Overseas travel is conducted regularly.
28	DISP is extremely laborious and complex for a small business.
29	Time to get clearances for team members especially NV1-PV.

Question 5:

Security compliance requirements limit your ability to be agile or innovative?

Strongly Agree	Agree	Neutral	Disagree
3	12	8	1



Question 6:

Please provide an example if you can

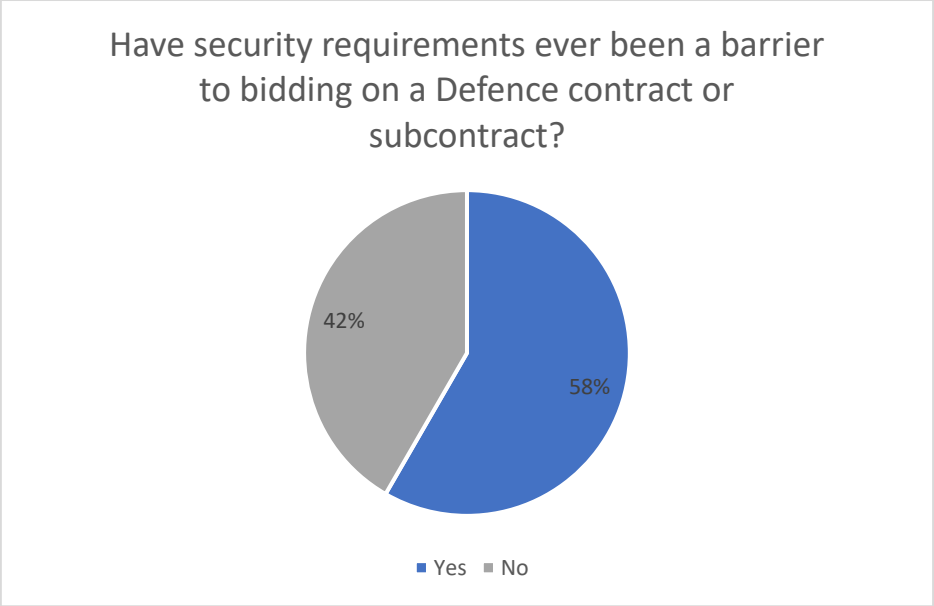
ID	Replace
2	Not doing multiple trial activities to advance our product offerings by gathering data because we weren't sure if it would be a breach of our security obligations. Employing multiple FTE to ensure compliance, where this effort could otherwise be directed to innovation.
5	Compliance is not necessarily the problem, particularly if it is a differentiator. We built defence "ready" systems for power and differentiated strongly against foreign manufactured goods. The problem is building and sustaining all the procedures, processes and operational friction that demand time, attention and effort when there is none to spare particularly when a substantial contract is yet to be landed and we can more readily deliver to industry than Defence.
6	Research often required working with third parties for their expertise, some of whom were not defence related companies but were specialised enough that we wanted to use them, not on actual equipment but clearly related to defence equipment.
7	Software development using randomised non classified data is obstructed by its intended end use.
8	E8 ML2 is difficult to implement for software development activities.
10	Again, processing delays.

ID	Replace
11	Regarding the Essential 8, I can give the example control "Adobe products are hardened in accordance with vendor/ASD guidance.". When you search for ASD guidance, it's non-existent. Adobe guidance again is similarly vague. I personally ended up adapting US DoD STIG guidance to meet this.
13	Trying to use machine learning or advanced AI tools to improve production processes, but you can't be the data relates to specific defence equiment being manufactured.
14	Regulatory compliance is only a problem when it directly conflicts with client direction. Otherwise it's just expensive.
15	We are a professional services firm and the compliance requirements imposed upon us, primarily DISP and other cyber security requirements, are not overly burdensome given our operational workflows. In my experience, where we see compliance requirements limiting agility of innovation it tends to be in companies undertaking software development, work in CAD products, etc - these users tend to require more flexibility and are impacted by tightened cyber security requirements.
19	The IT security restrictions are challenging to implement in an organisation that is doing design development
21	The extended time it takes for a system to be certified in order to interface with a Defence environment is deleterious to a fast moving technology enterprises needs. Our enemies generate technologies that interconnected and operational much more rapidly. The security requirements themselves are not the core issues, the core issue is the Commonwealths glacial pace for certification and accreditation assessments.
23	Speaking from the experience of clients, once technology products are reaching the stage of functional viability, the security requirements around managing supply chains, use of third party software tooling, and software development can hamper innovation. Sometimes Military and Defence security requirements are not keeping pace with changes in the market, although sometimes the threat models and security approaches can be different.
25	Whilst they're may be some truth to this statement, and I understand that security is often seen as the opposite to convenience, where you have a good, thorough understanding of what's required and how best to achieve it, i don't necessarily feel that this is the case. Yes, if you have little knowledge in how to properly secure an environment, you may go overboard and make it more difficult to be agile or innovative.
27	Considerations around physical security/location of assets.
28	We remain agile and innovative. Our ability engage with Defence in an agile and innovative manner is limited by many restrictions.
29	When running workshops to solve Defence problem sets we now are extremely limited in the use of secure facilities. Operating in these facilities significantly curtails access to internet, AI etc as well as receiving / outgoing calls. It’s literally like being cut off from the world. This is also not conducive to operating a business.
32	Agility = Speed. The time taken to review applications that could/should be deployed behind the DPN firewall is impeding speed to market and the implementation of efficiency measures.

Question 7:

Have security requirements ever been a barrier to bidding on a Defence contract or subcontract?

Yes	No
14	10



Question 8:

What changes or support would make it easier to meet Defence security obligations without stifling innovation?

ID	Response
2	More clarity and finer granularity.
3	Defence I think in a lot of cases need to understand the requirements themselves. there are regularly 2 different versions of the same issues depending what you read or who you speak with.
5	Everyone in Defence wants DISP accreditation visible at the time of Tender and will knock down the competitiveness of small business that does not comply regardless of whether the product is better. The same applies with achieved sales history and having a good size balance sheet. At D&I a senior leader stated Defence is not here to fund resolution of industry risk, that is a matter for industry. So the result is that only the primes and major medium businesses have the weight to carry such risk and any startups must access Defence through them. That means finding a prime with interest and willingness to tolerate and fund the risk.
7	A protected level centrally hosted by CoA defence industry network to provide flexible, efficient, timely, secure and auditable data sharing between industry, defence and government
8	Provisional DISP certification for new entrants (current DISP members meeting Top 4 for cyber are allowed to keep their DISP membership and go onto an uplift program. New entrants do not have this option.
10	Increased resources

ID	Response
11	Some sort of pathway or even grant to help smaller players participate and meet Defence security requirements. The scenario that comes to mind, is imagine a small start-up with say two people. The burden to become compliant is significant. The amount of policies / documentation that would be required, cybersecurity infrastructure (noting MSPs are an option), but I believe this is a barrier to innovation. It's a pay-to-play requirement that gatekeeps smaller organisations.
13	Common security obligations across AUKUS would be a great start, making DISP more like NIST where checklists are used to ensure networks are compliant. Having recognition that defence secruity is often lagging when it comes to innovation, so having ways that things like Machine Learning and AI can be used while still meeting defence security obligations
14	Eradication of US ITAR contamination by eradication of all US content in Australian developed and built product.
15	Expansion of the existing Defence Industry Development Grants program to further support industry to understanding their gaps against security compliance requirements and become compliant with them. Funding is available, however the scope of funding is limited in some areas such as security gap analyses (which actually provide organisations with understanding of where their gaps are and what they could or should do to become compliant). Education of procurement teams within Defence and Defence Primes around the level of requirements to be imposed across their supply chains and how to Replace questions/queries from prospective and existing suppliers around how to approach security requirements so they can appropriately support organisations with their security uplift and compliance.
17	Ability to access and use a common cloud environment
19	Produce better guidelines on implementation of ASD E8 Lvl 2
21	Increase the bandwidth of DCIAB by order of magnitude. Bring down assessment times for each system to NLT 2 weeks.
23	I think less time on expensive and inefficient assessments of Corporate Security, and some focus and support on security requirements for product development would be helpful - some times these additional service security requirements can be opaque and difficult to navigate, and if they are not known early they can waste companies time by making decisions to invest in architectures/processes and tech which wont meet the standards, and require extensive rework.
25	A consistent and well understood position coming from the top (including the Primes). Having some Primes mandate programs like DISP and others suggesting it is preferred does not send a clear message about the importance of security maturity in the supply chain, and provides enough grey area for some business leaders to turn their nose up at the investments required or defer these until some later stage (in some cases where it's too late...).
27	Flexibility in ITARs compliance/TPR through leveraging the AUKUS agreement vehicle.
28	Assistance in DISP application - happy to provide time and effort, but it is often overly laborious. We also provide software solutions, so authority to operate on networks is a challenge.
29	Defence has started to include sponsorship of attaining DISP on their contracts. This overcomes the financial burden and barriers to bidding on these contract.
32	We have individual staff that are/were cleared to higher levels than our Security Officer. This means that the company cannot secure work (even above the line/on Defence premises) for those individuals as the company is restricted to pursuing work at the highest level of the Security Officer.

Question 10:

Which parts of the procurement process create the biggest hurdles for your business?

Response	Qty
Response documentation burden	**5**
Tendering timelines	**4**
Pre-qualification requirements	**5**
Contracting terms and conditions	**1**
Security clearances	**1**
Use of MSPs and Primes without Competing work	**1**
MSP having 1st option at roles	**1**
All of the above!	**1**
CoA has a subjective view of policies and legislations.	**1**
Direct access to tenders	**1**
Slowness in approvals	**1**
Ambiguity of tender requirements and intent, with often contradictory or non-sensical clauses where assessed as a complete package	**1**
Other	**1**

Question 11:

Optional: What aspects of procurement do you find most challenging?

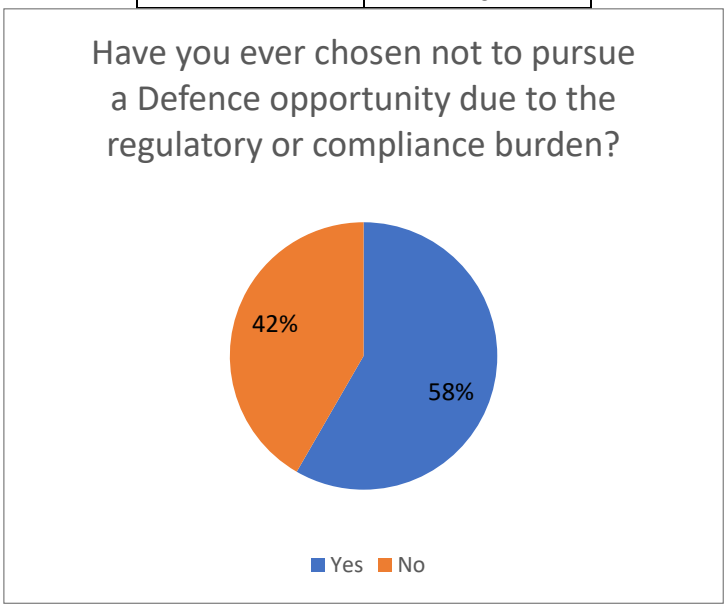
ID	Response
2	Short response timeframes limit the comprehensiveness of our offerings which creates risk as the project transitions to execution.
5	The problem for startup business that is innovative is that there is commonly no balance sheet, no sales and we are selling a creative idea to people who often don't get it, or if they do, do not accept the value / risk equation. Beyond that the challenges of getting a compelling written proposal to be understood with the head room for a dynamic two-way discussion is almost impossible. So the burden is both the weight of paper and the lack of meaningful engagement that can lead to understanding and creating of new forms of value.
6	We know that there are standard elements of defence contracts which we not agree to. Frequently these terms are flowed through from a prime's head contract which they have signed up to and expected us to just comply. Often these prime was not carrying out actual manufacturing or design and therefore the terms were not as relevant to them as therefore they accepted them but flowed them downwards. Intellectual Property, Liability, Insurance, clearance to engage third parties and unfettered access to both property and books are some of the critical areas.
7	Competing in an environment with demonstrably biased departmental acquisition executives that favour incumbency and their own industry job prospects upon separating
8	Responding to a complete ASDEFCON suite.

ID	Response
13	ASDEFCON, while these templates were created to simplify the process and allow tailored solutions to be created, Defence generally fails at tailoring, resulting in overly complex, overly burdensome frameworks that add cost and schedule to projects. Examples of similar risk/complexity projects in europe or the UK have under half the templates that the ADF use. When Govt seeks to make thing simplier, they should be removing siginificant sections of ASDEFCON, not adding more!
14	Defence staff not understanding Defence regulations. The conflict of interest created by Defence's Major Service Provider (MSP) contracts which allows MSP to exclude sub-contractors in favour of their own staff.
15	Working within Defence supply chains we often find tendering timelines to be the most burdensome, where we can sometimes be indirectly impacted if our clients or prospective clients are awaiting a Defence tender outcome before engaging us to support their security work.
17	Recent example: 1 month late to contract in time critical work package. No sense of urgency, financial delegation not held low enough. Standard practise is negotiating via email and with CoA commercial hiding from direct engagement and discussion.
19	Bullying behaviour by Defence and Defence Primes. Extremely short procurement timeframes often show that Defence has already made up its mind and is just going through the process. Different procurement frameworks and requirements for Primes and different areas of Defence
21	The application of CPRs varies across government.
22	For a SME, there is a large amount of pre-qualification, e.g. panels, security etc, requirements. And often, having completed that work, there is little access to work due to various CoA approaches to procurement such as the MSPs. These approaches are often the opposite of supporting Australian SMEs and a major challenge.
23	Time taken to make decisions, and inefficient timescales.
25	Dealing with professional commercial and procurement staff who do not fully understand what they're procuring or the importance of sovereignty of supply.
27	Poor requirements setting / disclosure, coupled with short lead times to respond. Repeated Approaches To Market with subsequent nil follow on action. Inability (or perceived inability) to present alternate solutions to RFTs for fear of having entire bids rejected.
28	Even if requirements are met in terms of technology and application, then having relevant security clearances, authority to operate and DISP are all additional hurdles.
29	Two of the above really. Response documentation can take weeks to put together. As an SME that’s a significant impact especially as probability of success is low. Responses to AUSTENDER takes this to another level. As an SME it is not worth responding to these tenders as ur competing against Medium to Large companies that have dedicated BD departments.
32	The MSP with hold roles in an attempt to fill them themselves before releasing them to the Technical Support Network for response at short notice after they have already swept the market.

Question 12:

Have you ever chosen not to pursue a Defence opportunity due to the regulatory or compliance burden?

Yes	No
14	10



Question 13:

Optional: If yes, how?

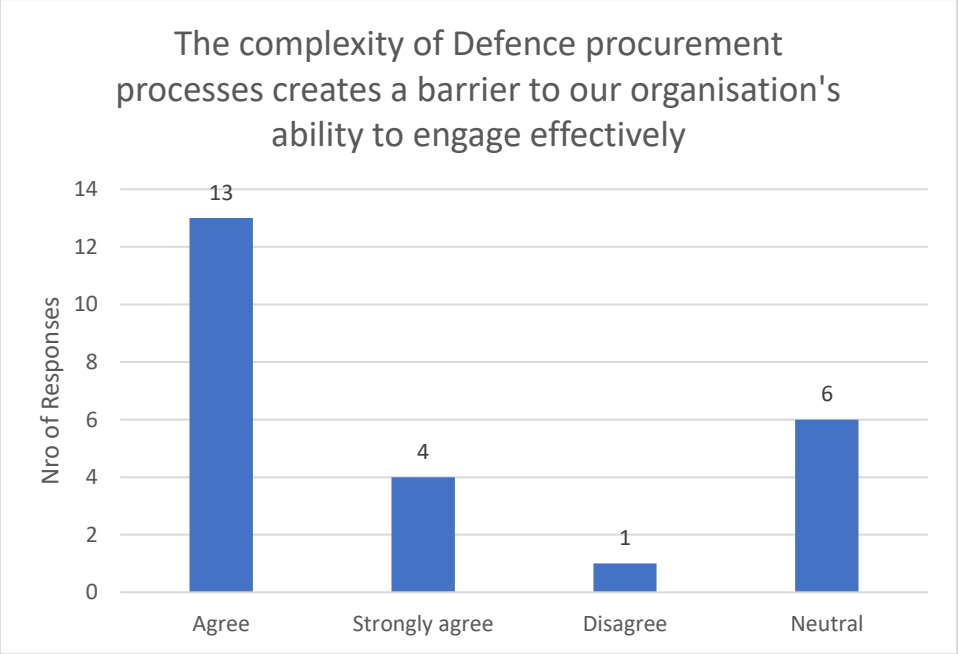
ID	Response
3	There is too much red tape for a small company to get through, often there is no value.
5	In way yes, the problem that small business has is trading off PWin against effort to be compliant and consistent with regulation. I have seen some great products that we just decided not to bother or to go in through an indirect approach through a prime. When they are good, primes can be great, but they too are bureaucracies and often are driven solely by their own business focus. Partly the challenge we have faced is meeting both Defence and Prime compliance standards which are not always the same or if they are, are likely expressed differently and submitted using differing systems.
6	We were of the opinion that a company had already been ear marked but there was a requirement for more than one proposal.
7	By simply not responding to a tender opportunity, or an invitation by RFQTS.
8	Deciding not to respond to RFIs and RFTs
13	Tenders released with massively complex compliance requirements, but then statements of work that ask industry to solve a poorly definced problem, which ultimately will make it difficult for anyone ot evaluate and compare different approaches in the proposal are normally unlikely to result in a contract so it is better to no respond.
14	The requirement for compliance creates opportunity. We sell compliance with Defence regulation and we're good at it..
22	If the opportunitity and submission requirements do not align we will not proceed, e.g. for a small opportunity there is a large requirement for submission, both in terms of submission requirements and supporting compliance documentation.

ID	Response
23	We are deliberately working below the line, so we do not need to get on the larger proposals.
25	Sometimes the return on investment is just not there, and we decide to "no bid" the opportunity in favour of opportunities in other sectors or direct with industry.
26	Not submitted a response to a tender
27	Mandated requirement to be on a specific Defence site, that was not related to the performance of the duties/delivery of the outcomes.
29	We chose not to bid on a AUS tender, even though we could have added a huge amount of value, when we saw there were 100s of companies in on the industry briefing
32	Roles that our staff are suited to, but their clearance was limited to that of the company SO.

Question 14:

The complexity of Defence procurement processes creates a barrier to our organisation's ability to engage effectively

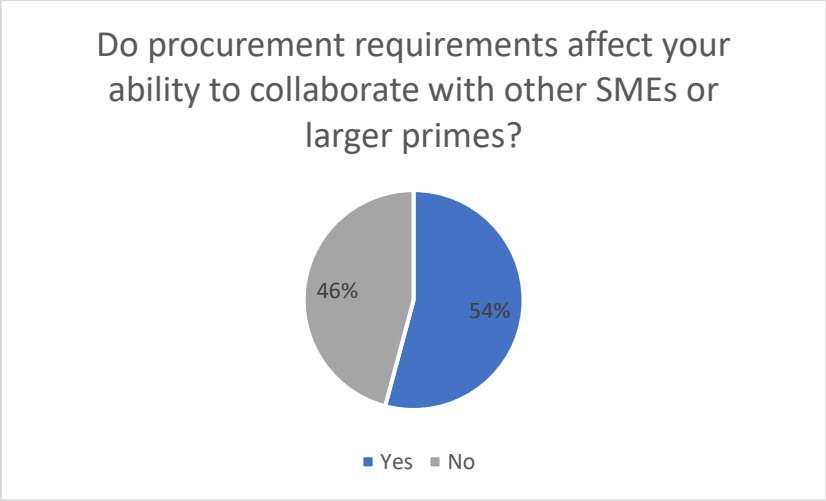
Strongly Agree	Agree	Neutral	Disagree
4	13	6	1



Question 15:

Do procurement requirements affect your ability to collaborate with other SMEs or larger primes?

Yes	No
13	11



Question 16:

Optional: If yes to question 15, how?

ID	Response
5	This is kind of a yes. The real problem is that we are often walking in fog and don't really know what the driver for other parties is, while at the same time we are trying to protect our commercial advantage in a very competitive world. Often the big hurdle is probity preventing meaningful engagement without giving away trade secrets when responses are shared publicly back through the portal.
7	Chicken and egg, where collaboration requires pre-approval, but without negotiating the subject, the feasibility and terms are unknown prior to engaging in lengthy demonstration of compliance
8	Larger primes flow down all T&Cs (including IP clauses, indemnity clauses etc). They flow down all the risks and keep much of the rewards.
12	Use of MSPs seems ineffective, and inhibits fair competition. The MSPs do not put all available work to their network, instead they frequently offer their own inferior staff or staff on the bench. They also use their unfair advantage of knowing our rates to undercut. This is unethical.
13	Primes, rather than managing risk they attempt to offload as much as they can to suppliers or sub contractors. ADF needs to either reduce the burden place on the Prime, or limit what can be flowed down to sub contractors. A sub contractor can't reasonably be expected nor should it be asked to agree to unlimited liability or $100m worth of liability if it is only providing $3m worth of equipment onto a ship.
14	If there's not requirement to procure there is no opportunity to provide regulatory compliance.
15	As above, we are from time to time impacted by tender processes our clients are going through before they can engage us, this can impact our sales cycles and ability to resource engagements effectively.
19	Indirect restrictions on collaboration with other SMEs. Defence preference to always favour a Large international company over an Australian SME or Prime
22	All primes have different requirements and processes as there is not a standard, further complicating it for SMEs.

ID	Response
23	It is a cost to business - sometimes we will defer participation because of the costs involved in making a decision.
26	Affects business relationships
27	Sometimes, the manner in which some RFQTS hit the market limit the ability to team with other players. Increasingly tight turn around times limit the opportunity to effectively collaborate.
28	Often as a SME, we may partially meet requirements, but not all requirements of a tender. We are very willing to work with other companies, but it is almost impossible to know who fills in other areas of a tender, so a partial response, if often ruled out (or we don't respond).

Question 17:

Do you believe current Defence compliance expectations encourage or inhibit innovation in your business? Why or why not?

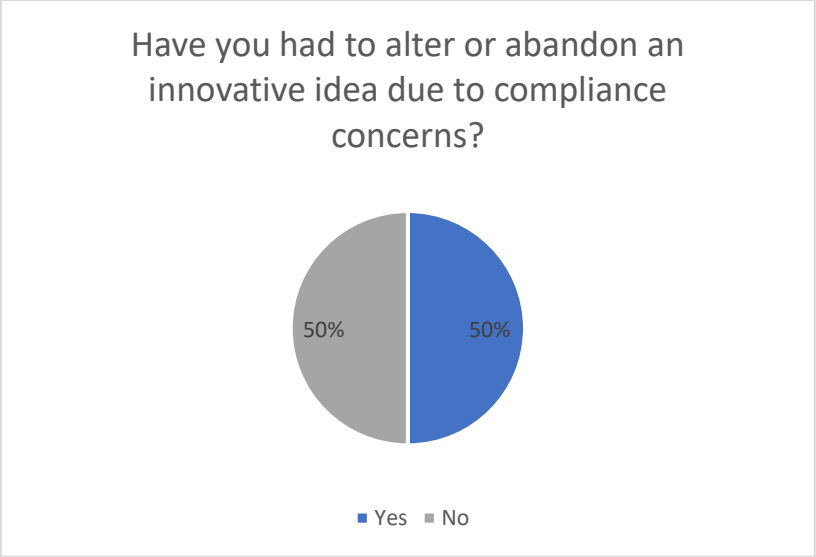
ID	Response
2	Like any business we have finite resources. Any capacity that is not required to meet our non-negotiable obligations is focused on innovation. By directing multiple FTE to compliance, that is head count that could have been used to innovate.
3	It's inhibited by the time it takes to gain approvals even temp approvals take too long
5	They will always inhibit innovation because they are a natural handbrake purported to protect the procurement effectiveness, but mostly just protecting public servants from being tested for their professional behaviours and enabling them to avoid having their decisions reviewed.
6	Generally inhibit normally because of the inability to directly engage with Defence/CASG.
7	Inhibit. It is costly and redirects time and money from R&D, beyond what is necessary. Often processes to comply with have been invented simply to satisfy another process.
8	Yes. Reliance on T&M, labour rates (even in ASDEFCON tenders) encourages a people centric solution and discourages adoption of innovative solutions such as AI, process improvement, alternative solutions etc.
10	While the good intent behind Defence compliance frameworks is to strengthen security and accountability, in practice, the extended delays in processing timeframes...whether for security clearances, DISP applications, or export controls, can significantly inhibit innovation. For businesses operating at the cutting edge of technology or product development, the ability to move quickly is critical. Long compliance related lead times can delay recruitment of key personnel, slow project initiation, and create uncertainty around timelines...all of which hamper agility and responsiveness. In a sector where speed-to-capability and first-mover advantage matter, this lag can result in missed opportunities, both domestically and internationally. Innovation thrives in environments that are both secure and responsive. The current system, while well-intentioned, needs greater efficiency and clarity to truly support innovation at the pace required in modern Defence industry environments.
11	I would say hinder. I look from a cybersecurity perspective, but novel ideas can quickly run into "yes, but that requires these resources to be secure and compliant.". A small idea that may pursue a prototype or even proof of concept can quickly turn into an expensive exercise, particularly for smaller organisations.
13	In the Australian context, yes. Plus if you are innovative who are you selling it to, ASCA is really only looking at high maturity level technical solutions where they know what the solution looks like.
14	No. See Q12.

ID	Response
15	They probably actually encourage innovation in our business given we work with clients to support their security uplift and ongoing compliance. Our team is constantly reviewing security compliance requirements as well as products or services that can be used for compliance. We are also innovating and developing our own products and services to better support companies to understand and meet their requirements - specifically technical services, consulting services, training and education.
17	Issue is mandating new requirements (eg nuclear ISO19443) before understanding if current systems processes certification is good enough
19	Discourage. There are sometimes excessive security requirements on roles, and a requirement for staff to be based in Canberra, due to not having classified facilities available for SMEs to work from in other capitals or regions.
21	Defence compliance expectations encourage innovations to be sold overseas to foreign militaries. This is because of the risk based view CoA uses to via DSTG to asses new capabilities. Industry are incentivized to sell technologies overseas in order to be viewed as lower risk to the CoA.
22	Inhibit. Due to the specific nature of Defence business and security requirements, often rightly so.
23	To be honest, it encourages to be innovative, because we are trying to come up with ways to help our clients meet security requirements in the most efficient way possible! However, it would be better if some of the compliance requirements were managed more efficiently by Defence to increase the speed that organisations could reach the market.
25	Neutral. We always find a way to innovate and do it differently. It's a level playing field, so we only need to be as innovative as or slightly better than the next company looking to service Defence. Could we be more innovative in another sector? Probably, yes.
26	It is improving
27	Yes, compliance concerns around what some members may perceive as conflicts of interest. This is inherently a personal assessment and it is not common across organisations or members of staff. This makes it difficult to commit to activity that may be perceived as a potential conflict of interest, for fear of losing other work.
28	Inhibit - just the general overhead of compliance on a small business is high. I understand the need, but often Prime requirements and a broad application to SMEs as well. For example, no we don't have a modern slavery policy ... but it's often a requirement.
29	Yes and No. we are working on reducing these compliance barriers by better educating Defence on how much is enough especially around technical compliance.
32	Once an SME has navigated the requirements it provides access opportunities that competitors may not choose to work through. While good for Defence experienced SME, this is not in the interests of Defence as it has artificially limited the market.

Question 18:

Have you had to alter or abandon an innovative idea due to compliance concerns?

Yes	No
12	12



Question 19

What would a more innovation-friendly environment look like to you?

ID	Response
2	Clearer obligations and outreach to reduce the burden on industry to interpret and comply.
3	Defence being more agile with contracts and requirements
5	More like RPDE where we could have a good open, but protected discussion and no body had their career at risk and IP arrangements were in place to enable safe collaboration. When we sacked RPDE we lost something very important due to ill judgment.
6	Have better or more open conversations. Some primes would not consider innovation as there was a cost involved with them to push the idea upwards as well as changes to documentation or drawings. For those involved in the middle it was easier to say NO.
7	Ability to interact and experiment within a security assured sandbox, rather than repetitively demonstrating compliance for each and every initiative or opportunity.
8	A different procurement arrangement where improvements are shared and less reliance on pure T&M.
10	An innovation friendly Defence environment would maintain strong compliance standards but deliver faster, more predictable processing...particularly for security clearances, DISP, and export permits. A tiered, risk-based approach would help reduce bottlenecks for lower-risk projects, while clearer guidance and better communication would support faster decision-making, especially for SMEs. Support for dual-use technology pathways and more structured collaboration between Defence, industry, and academia would also drive innovation. Ultimately, innovation requires agility, not unnecessary delays. Faster, clearer processes would help businesses move at the pace modern Defence challenges demand.

ID	Response
11	Again, from a cybersecurity point of view. Some sort of path-way or sliding scale for smaller-medium organisations to even get involved. As an idea, an Australian Gov Cloud environment that DISP applicants/members can operate out of. There would be some sort of fee, but it could significantly reduce the barriers for entry for smaller organisations and startups.
12	More Money for good ideas, more acceptance of risk by the Commonwealth.
13	An environment where Defence defines the problem it wants solved, rather than what the solution should look like. Industry then has access to rapidly progress technology through TRL with operational environments provided by defence.
14	Defence project managers being able to determine what constitutes value-for-money rather that being constrained to expend project funds through the MSP contract(s).
15	Better collaboration between Defence / Defence Primes and SMEs to work together to achieve compliance requirements. Consultation from Defence/Primes with SMEs when they are developing compliance requirements.
19	One where Defence was more willing to take a chance on an Australian SME, owned and managed by a Defence Veteran. Clear and consistent timeframes for tenders. Better visibility on contract awards and contract extensions, with written summaries of tender evaluation reports made public. More open competitions, not Defence assuming that it can pick the winner. Don't overrate the ability of a Defence Prime and underrate the ability of an Australian SME.
21	It would require the Commonwealth to develop the capacity to "Try it out and see".
22	Commonwealth actively implementing and managing actual opportunities for Australian SMEs to grow the ecosystem.
23	Some of the standards around security should be more opaque. Corporate security requirements are better known but ineffeciently assessed. More information and advice around security in actual products and technology would be more useful.
25	Less paperwork/commercial T&C's which lock you in to certain performance targets. More willingness to see a larger number of innovative projects fail and more investment in Australian technology companies / products. A lot of this comes down to the media in Australia though, who crucify Defence and any companies involved in these projects when they do go bad/not as intended.
26	Smoother regulatory compliance processes, greater transparency in procurement, better panel arrangements for SMEs & access to R&D grants
27	Take a leaf out of USG and SOCOMD books with the "Fail fast/early approach". Without risk there is less chance of reward, and the timeliness of capability delivery is actively hampered by the total risk aversion exhibited by the ADO wrt SME's.
28	Smaller oversight during engagement, with a sliding scale to assist with security and general compliance (i.e. IS9001 / ISO9100 etc)., as project / engagement evolves.
29	A blended workforce of defence, industry and academia co creating solutions to Defence problem sets
32	New technologies are heavily reliant on IT (AI/LLM). The inability to deploy versions of these tools within the DPN where they draw only on data available within the domain is reducing efficiency and opportunities.

Question 20:

Would you be open to participating in a follow-up, face-to-face interview to share your story as part of a case study?

Yes	5
No thanks	13
Maybe - Please contact me with more info	6