babcock™ **Babcock Pty Ltd**

Level 9, 70 Franklin Street
ADELAIDE
South Australia 5000
AUSTRALIA

Postal Address:
(GPO BOX 1275, Adelaide)
(South Australia 5001)
(AUSTRALIA)

Tel +61 (0)8 8440 1400
ABN 50 011 075 460
www.babcock.com.au

27 October 2022

Committee Secretary
Joint Standing Committee on Foreign Affairs, Defence and Trade
PO Box 6021,
Parliament House,
CANBERRA ACT 2600

via email: jscfadt@aph.gov.au

Dear Committee Secretary,

Babcock Australasia Submission to the Inquiry into the Defence Industry Security Program Auditor-General's Report

Babcock thanks the Joint Standing Committee on Foreign Affairs and Trade for the opportunity to make a submission to its Inquiry into the Defence Industry Security Program Auditor-General's Report. The Defence Security Industry Program (DISP) is one that Babcock considers as essential part of the package of measure that ensure Australia's Defence Capability is strong now and into the future. The opportunity to contribute to its improvement is something that we consider is an obligation upon us as a Defence Prime.

As a long-standing member of the DISP, our submission has been compiled to consider the underlying causes of issues we have identified, rather than provide commentary on each of the recommendations made by the Australian National Audit Office (ANAO) in their report. We therefore wish to bring the following observations and recommendations to the Committees attention:

1. Defence Industry Security Program

Defence needs to adjust its understanding of the context in which the DISP operates. The program has been long been focused upon replicating the delivery of a compliance structure as it is applied upon the various units within the Department of Defence. It is within this context that the construct of the documentation and procedures used by the program have been developed. While this has been able to show surface level of results it fails to acknowledge that many of the aspects that make artifacts such as 'Security Policy & Procedures' and 'Facility Security Registers' that are inadequately constructed to meet the needs of DISP members as they do not work within the same context.

The Defence environment, even in the civilian areas, works within a defined Command/Management structure that is supported by the wider Defence Information Management Systems, Insider Threat programs, data collection/analysis, and various other services provided by the groups/services. All of which do not exist in the same environment, legislation, or delivery objectives as those that the DISP membership operate in. Therefore, many of the medium to large DISP members create and maintain these artifacts only for the purposes of meeting the limited audits that focus on the compliance of having an artifact rather than having an effective tool by which the DISP member can collect and analyse data with the purpose of maturing its Protective Security environment. As a result, Defence is unable to understand if the larger organisations, with a much greater level of aggregate risk, are managing those risks beyond the basics that would be expected from a much smaller organisation.

This approach does not remove artifacts that are needed as an exemplar for smaller members, while accepting that medium to larger organisations will need to be allowed to develop their own tools.

A move towards a guided maturity model of assessment would be a far more effective means of assurance that the aggregated risks of the DISP membership are being managed. This type of maturity modelling is difficult and requires a high level of skill and knowledge in the application and management of Protective Security by both the user as well as the assessor. Unfortunately, this is not widely available to the Defence Security & Assurance Branch (DSoA) or with the Protective Security capability of most DISP members.

Recommendation 1:

DISP move toward a guided maturity model of assessment to provide a more effective means of management assurance of the aggregated risks of the DISP members.

2. Education and Training

This brings us to the single largest cause of the problems within the DISP, that of the education. With the demise of the foundational training that was provided by the Protective Security Training College, Attorney General's Department (PSTC) and the move of the other tertiary providers towards a more Cyber/Information Technology focus, the profession has become reliant on mentoring as a means of training the next generation of Security Advisors and little to know training for managers.

As a result, we have seen the situations in DSoA where the advice provided by the various State/Territory Offices differs greatly. This has created challenges in obtaining clear advice, seeking advice beyond established policy, risk assessments that have taken an evidence-based assessment and documentation that relevant and tailored to the operations. An example of these challenges can be found in the compulsory Security Office, which appears focussed on the completion of a Facility Security Register and delivered by facilitators with limited operations experience.

If the DISP is to meet the expected improvements from the recommendations made by the ANAO, it is in the building of the skills and knowledge of those responsible for their implementation where the most significant value will be achieved.

A potential approach would be to build a strong educational program that has a range of packages available to both members of the DSoA as well as Security Advisors within the membership. These packages must not just cover the basics but look to upskill in the key areas of:

- Physical and electronic security so that members can contribute to the Security by Design of these aspects as controls within their organisation rather than an overreliance on to not just take manufacture and Security Zone Consultants recommendations.
- Capacity to develop internal intelligence gathering tools, analysis, and development on education programs for their organisations so that they can manage their insider threat.
- The foundational skills that develop the information that drives risk assessments, particularly in the areas of Critical Function and Critical Resources Analysis.

DSoA has in the past attempted to build and deliver individual training courses that have been unable to deliver on objectives due to their construction, subject matter expertise challenges and a difficulty aligning policy, content, and the expectation of capability when delivered in operational environments.

As a solution to overcome this situation it is worth looking at the model used by the Services in their trade/employment schools. These schools have a core of experts in the development of educational programs and packages which can then draw upon Subject Mater Experts (SME) from within Defence and the wider DISP membership.

The benefits of this are that it would allow all parties to draw upon a wider based of knowledge and experience, particularly in the operational areas. They can also move away from an 'attendance' model and move to one that deems a participant as Competent/Not-Competent based upon a robust assurance model that ensures the training is valued by the community. The model can look to utilise a cost recovery program that benefits the DISP membership by acknowledging the provision of support by offsetting the cost of courses so that it does not have a significant budgetary impact on either of the parties.

I would note that like many of these schools there is no need, or value, to moving towards a Registered Training Organisation (RTO) that aligns with Certificates/Diplomas. To do so would only limit the education benefits as the Government (Security) qualifications do not adequately demonstrate of what is required by members of the Protective Security profession and would reduce the flexibility to create, improve and direct course content to areas of need. This is highlighted by the fact that at the height of its operations, the PSTC only 1 in 3 delivered courses were based upon RTO qualifications. The quality of the education package can be maintained by having a peer group, whom would also be your base of SMEs, who could ensure that content and assessment models are effective in delivering quality participants.

Recommendation 2:

A suite of strong educational programs be designed to equip DSoA and Security Advisors within the membership with adequate skills and knowledge, that can be tailored to their circumstances.

With these aspects of change in place it generates the capability to move the DISP towards a maturity, rather than compliance, model of assurance. This model can then look to focus on assessing the ability of the organisation to provide an effective Protective Security environment using a structure that suits how it does business and not how Defence conducts itself.

Babcock acknowledges that the paradigm shift in the delivery of the DISP would not be easy for any of the parties involved. However, we are currently positively working with DSoA as an able partner and will continue to do so into the future towards a more effective and robust DISP that will see a stronger and more capable Defence Industry.

We are able to provide any further information the Committee may require on matters covered by this submission.

Yours sincerely,

[redacted]

James Jordan
National Security Manager
Corporate Services | Australasia
[redacted]