Wednesday, 2 November 2022

Committee Secretary
Joint Standing Committee on Foreign Affairs, Defence and Trade
PO Box 6021
Parliament House
Canberra ACT 2600
jscfadt@aph.gov.au

Dear Committee Secretary,

Leidos Submission to the Inquiry into Defence's Contract Administration – Defence Industry Security Program

Leidos Australia welcomes the opportunity to provide a submission to the Joint Standing Committee on Foreign Affairs, Defence and Trade's Inquiry into the Defence Industry Security Program Auditory-General's Report.

This submission reflects Leidos' appreciation of the Defence Industry Security Program (DISP) and its efforts to achieve Defence readiness. As a DISP accredited organisation and key supplier to the Department of Defence, Leidos is well positioned to acknowledge the successes of the current Program and suggest areas for improvement.

We urge the Committee to consider the recommendations contained within the enclosed submission and would welcome the opportunity to present or clarify any of our recommendations with the Committee in further detail, should the opportunity arise.

Should you have any further questions, please do not hesitate to reach out.

Yours sincerely,

[redacted]

Paul Chase
Chief Executive

Leidos Australia
ACN: 612 590 155

Table of Contents

1 Introduction

Leidos Australia welcomes the opportunity to make a submission to the Joint Standing Committee on Foreign Affairs, Defence and Trade's (the Committee's) Inquiry into the Defence Industry Security Program Auditory-General's Report.

With 25 years of local experience, Leidos Australia is working to solve the world's toughest challenges in government, defence, intelligence, border protection, and health markets. We employ more than 1,500 local experts who, backed by our global experience and network of partners, deliver solutions that help secure Australia and make the world safer, healthier and more efficient through information technology, engineering and science.

Leidos is a FORTUNE 500® global science and technology solutions and services leader, reporting annual revenues of approximately US$12.3 billion in FY21. Over the past half-century, Leidos has worked in some of the most advanced areas of science and technology to deliver critical solutions to our customers' most demanding challenges.

We deliver for the Australian Government in every state and territory, supporting the Department of Defence, the Australian Defence Force, the Australian Taxation Office, the Bureau of Meteorology and Australia's National Intelligence Community in delivering solutions in information technology, cyber, systems integration, and chemical, biological, radiological and nuclear protection.

Leidos Australia is a Defence Industry Security Project (DISP) organisation operating numerous accredited classified facilities and ICT systems. These are located throughout Australia for Projects including Joint Project (JP) 2030 Joint Command Support Environment, and Chief Information Officer Group (CIOG) Central Processing (CP). Leidos is fully compliant with all Defence Security Manual and Information Security Manual requirements, as well as all other aspects of the Commonwealth's Protective Security Policy Framework.

Leidos has established and continue to operate Sensitive Compartmented Information Facilities in support of numerous classified Projects. We have experience over more than 15 years establishing, operating, and accrediting Defence classified networks at the Protected and Secret levels. This wealth of practical project experience attests to a mature existing capability that will continue to improve and be applied to future Commonwealth projects.

Due to our long history supporting the Department of Defence and as a DISP member, Leidos has a vested interest in the uplift and effectiveness of the DISP. Accordingly, we have developed this submission for the consideration of the Committee in its review of the Report.

2 Summary

There are many synergies between Leidos' experience with the DISP, and the findings of the Auditor General's Report. Leidos would like to express support for these findings and recommendations, and put forward further considerations and evidence for the Committee to outline inefficiencies of the DISP.

Foremost, Leidos would like to acknowledge the significant improvements made by Defence to refresh the DISP for 'Defence readiness'. Industry has seen a transition to an easier process of doing business with Defence, supported by the impacts of the following successes:

1. The ability for self-sponsorship of clearances. This initiative helps industry to maintain cleared personnel prior to winning a contract and in non-delivery roles without a program sponsor, both of which were previously problematic for industry, particularly small-medium enterprises.
2. The requirement of a whole of business Chief Security Officer (CSO) and Security Officer (SO) for each member company. This provides single points of contact and has assisted with engagement between industry and Defence.
3. Increased availability of helpful resources for members. The availability of these resources are very important for organisations new to DISP, however more are required.

Despite these significant improvements, there are a number of challenges still facing industry, defence and the DISP program. These include:

1. Lengthy processing times for clearances. Although we have seen professional and helpful service delivery from AGSVA and the SICC, the lengthiness of clearance processing is a key barrier to delivering to Defence. Additional resources were required for the first few years from introduction to manage the volume, and Defence would still benefit from the allocation of these resources.
2. Although centralising governance and reporting is less effort for industry, there is still a number of bespoke reporting requirements for different contracts, which requires additional resourcing and decreases the quality and efficiency of communication due to unfamiliarity with processes.
3. We have received sound advice from Defence Security and Vetting Service (DSVS) on achieving and maintaining DISP compliance, though some aspects of DISP require more direct guidance,

at least for minimum standards, one area of particular concern, where advise is lacking, is the insider threat program requirement.

4. Defence does not complete due diligence to a level acceptable by industry in application to the DISP, predominantly due to the lack of requirement for evidence or follow-up in the application process. A Third Party Supplier holding a DISP membership does not necessarily provide adequate assurance to Leidos in terms of assessing our supply chain to meet the requirements of Defence contracts in relation to program security and security flow-downs to subcontractors, due to either a limited follow up on DISP applications post approval, or to enhanced security requirements in contract which do not align to the DISP program requirements. While this is not a core tenet of what DISP is required to provide, it is concerning that this membership, externally can fail to provide confidence of a business' ability to adhere to Defence requirements and manage the risk to Leidos flowed through from the head contract.

3 Recommendations

Leidos proposes the following four recommendations to ensure continual improvement of the DISP, ensuring efficiency of resources, communication, and delivery:

1. **Defence should endeavour to educate and advise on changes in requirements better, both internally and with industry to ensure consistent advice and outcomes.** Improved communications from Defence when changes are made will ensure due diligence requirements and reporting are consistent and fit-for-purpose.
2. **Defence should invest in comprehensive training for internal DISP resources.** This would ensure Defence readiness is at the forefront of the procurement process, and further cover Project Management training, specifically the impact of lengthy processes on delivery schedules. Notably, it is not possible to identify and build an accredited facility and operate Defence networks from it in less than 12 months. A method for self-accrediting to Zone 3 or 4 and DSE would help alleviate this.
3. **Defence should increase due diligence practices in DISP application processes** to ensure accreditation is fit-for-purpose and creates benefits across industry.
4. **Defence should work to improve communication to DISP members through the stand up of a DISP Member Portal and dedicated points of contact** within DISP for each member. Defence should develop uniform guidance on DISP requirements and changes to be distributed through

these centralised channels of communication as well as an avenue to allow members to advise change of circumstances through this portal that may impact their DISP membership.

4 Conclusion

In conclusion, although Defence has made significant improvements to the Defence Industry Security Program, there are a number of key challenges that disrupt the achievement of desired outcomes under the Program. Leidos would like to highlight our support for the Auditor-General's six recommendations to improve the management of DISP requirements, compliance, and non-compliance and we express our gratitude for the opportunity to put forward further recommendations outlined in this submission. Leidos recognises that through dedicated efforts to increase training and due diligence practices, efficiency of communication between Defence and Industry, and centralisation of compliance efforts, DISP will continue to develop towards a fit-for-purpose Program that enables Industry to best support Defence in defending Australia and its national interests.