Australian Government December 2024 Update to the Joint Standing Committee on Foreign Affairs, Defence and Trade report:

The Defence Industry Security Program
Review of Auditor-General Report 4 of 2021-22

Recommendation 1 *The Committee recommends the Department of Defence provide written advice to the Committee within six months of the tabling of this report detailing the implementation of the Customer Relationship Management (CRM) system, how it assists with knowledge management and engagement with DISP entities, and its ability to recall accurate, auditable, and accessible data on DISP entities.*
No update required. Recommendation 1 was completed in June 2024.
Recommendation 2 *The Committee recommends the Department of Defence listen more carefully to industry concerns raised via this inquiry regarding the quality of DISP security training including for APS staff and embed a structured, transparent mechanism to ensure industry feedback directly informs continuous improvement to ensure training meets industry's reasonable expectations.*
No update required. Recommendation 2 was completed in November 2023.
Recommendation 3: (a) *The Committee recommends the Department of Defence implement systems which regulate and audit DISP compliance, and:* • *Within **six months** of this report being tabled in Parliament, outline in writing to the Committee how all six recommendations of the ANAO in Auditor-General Report No. 4 of 2021-22 have been fully implemented, and any actions which remain outstanding.*
No update required. Recommendation 3(a) was completed in June 2024.

Recommendation 3: (b)

The Committee recommends the Department of Defence implement systems which regulate and audit DISP compliance, and:

- *Within **twelve months** of this report being tabled in Parliament, report back in writing to the Committee on its progress in further improving DISP related compliance and audit systems and provide reliable data estimates of:*

1. **The number of contracts that require DISP membership and the classification levels required.**

2. **The number of contracts which did not, but were identified as requiring DISP membership, the classification levels required, the dates the contracts were entered into, and any action taken to address these.**

Defence undertook a data governance and management uplift within Defence Industry Security Branch (DISB) that included establishment of processes and a Customer Relationship System (CRM) in alignment with Defence enterprise data policies and standards.

The CRM includes a Reporting and Analytics capability which is able to recall accurate, auditable, and accessible data on DISP entities that provides reliable, timely and consistent information and insights. As detailed in **Annex C,** further maturing of data and integration will continuously improve the accuracy and quality of DISP data and reporting.

A DISP Data Governance and Reporting Framework was developed to provide a clear description of roles and responsibilities, define the lines of authority and outline baseline data processes and associated controls. The Framework formalises data quality management and ongoing monitoring of DISP membership and contracts data and data sharing arrangements with other parts of organisation.

As a result of these initiatives there has been substantial improvements in integrity, reliability, availability and security of the DISP membership data, addressing key findings of the ANAO Audit. Accurate DISP membership and entity data is now more readily available for key programs and executive decision-making.

For the period July 2023 to October 2024, approximately 4,000 contracts classified at the OFFICIAL level that require DISP membership have been identified and recorded in the DISP Membership System (DMS). These contracts have been identified across key systems using their Australian Business Number (ABN) and matched with existing DISP members and Applicants.

A further approximately 5,000 contracts classified at the OFFICIAL level have been identified that potentially may require DISP membership according to information reported by contract managers to AusTender. Defence is maturing processes to review and validate these with contract managers for accuracy in reporting to AusTender and assessment against mandatory DISP requirements.

As at 6 November 2024, there are 131 active contracts classified above OFFICAL for DISP Members and Applicants.

Data caveats, sources, systems, and methodology used to derive reported contracts information can be found at **Annex A**.

Future improvements to Defence contracts data can be found at **Annex C**.

3. **The number of contract managers that manage contracts with mandatory DISP membership.**

4. **The number of these contract managers who have received training in managing contracts with DISP memberships and how many contract managers lack required training.**

As at 29 October 2024, the number of potential contract managers identified responsible for managing open contracts with DISP Members and Applicants is shown at *Table 1*.

DISP Membership Status	Number of unique contracts	Number of Unique Contract Managers
Members	20,158	5,257
Current Applicants	2,664	1,404

Table 1 DISP Member and Applicant Contract Managers

Data caveats, sources, systems, and methodology used to derive reported contracts manager information can be found at **Annex B**.

The Defence Security Service Offer has been refreshed to provide contract and project managers with comprehensive information on accessing DISP support and tools.

The Commercial Skilling Framework has incorporated DISP into the framework and embedded information on DISP into the Defence Procurement Manual. Specific policy guidance and training for contract managers and security personnel engaged in defence research and collaboration has been developed and is being implemented.

Due to the broad training on offer to contract managers, it is a challenge for Defence to obtain numbers specifically attributed to DISP membership, although it should be noted that essential contract manager training offers have been updated to include DISP information and guidance, including maintaining contract DISP security obligations.

The ability to report on DISP contract manager numbers, as well as effectiveness of training, is part of the DMS integration and reporting roadmap into 2025 – 2026.

Defence has enhanced and implemented a number of actions to uplift DISP contract manager engagement and training. Further information is outlined in this report at **question 6**.

5. **What ongoing mechanism is in place to ensure staff receive the required training in the future**

Following the successful implementation of DISP Security Officer training, DISP will replicate this modularised approach to develop updated DISP contract manager training commencing in Q1 2025.

In addition, DISP will continue to work with Capability Acquisition and Sustainment Group (CASG) to refine training requirements as part of essential contract manager training offers; engage with

contract managers on training as part of the DISP Out Reach program; and update DISP contract training on the new DISP Contract Manager Portal released in September 2024.

6. How Recommendation 2 of this report has been implemented.

Recommendation 2
The Committee recommends the Department of Defence listen more carefully to industry concerns raised via this inquiry regarding the quality of DISP security training including for APS staff and embed a structured, transparent mechanism to ensure industry feedback directly informs continuous improvement to ensure training meets industry's reasonable expectations

As previously covered, Defence has implemented a number of actions to uplift DISP engagement and training

a. **Engagement:** DISB successfully hosted its inaugural DISP Industry Forum on 17-18 June 2024 with over 600 Industry members attending day one and 400 contract managers attending the second day of the forum. The second day focused on contract managers, including sharing of key information on the program and their role in managing security risks under contracts. DISP have also introduced a contract manager newsletter to keep contract managers informed of key policy and program updates. DISB have also engaged with Industry and contract managers at major events including Land Forces and Australian Defence Science Technology and Research (ADSTAR) in September 2024 and has supported Office of Defence Industry Support (ODIS) and Australian Government Security Vetting Agency (AGSVA) on roadshows.

b. **Training:** DISB successfully released its new modular, on-line DISP Security Officer training and plans to approach the market to refresh the existing DISP Awareness Course for contract managers. The new training package will be co-designed with contract managers and consulted with industry to ensure it is fit for purpose. The design-phase is scheduled to take place in the first half of 2025, with the build-phase planned for Q2 2025/ Q3 2025, and the pilot launching in Q3 2025.

c. **Support:** DISB has established a complex case management team, increasing support for contract managers on complex cases such as non-compliant DISP members, members with high Foreign Ownership Control or Influence (FOCI) risks, and Universities.

d. **DISP Assurance:** Implementation of the DISP Assurance Criticality and Escalation Framework to support timely and consistent escalation of security risks and non-compliance is complete. The framework includes mechanisms to ensure that contract and capability managers are aware of industry security risks within their remit.

e. **DISP Membership System (DMS):** Capability Release 2 of the DMS went live on 30 September 2024 allowing DISP members to complete their Annual Security Reports (ASR) and the uplifted Cyber Security Questionnaire (CSQ) on-line from 30 September 2024. The release also introduced a new Contract Manager Portal that digitised the current contract manager touchpoints in the DISP process through retirement of the AE250-2 (DISP Contract Notification) form and improved reporting for contract managers.

f. **DISP Decision Tree**: Assists contract managers in determining when DISP membership is required, explain the security benefits of DISP membership, and reinforce the need for contract and project managers to manage security risks specific to their contracted activities.

g. **Defence Direction:** Is provided to all contract managers through Policy, including the updated Defence Security Principles Framework 16.1, to include DISP membership clauses where required in new contracts; determine if DISP clauses are needed in existing contracts; ensure contractors hold and maintain required levels of DISP membership; and confirm appropriate measures are being taken to address any potential DISP non-compliance.

h. **My Procurements System**: Enhancements to the contracting tool to support Defence officials in determining if the scope and security risks associated with a procurement requires a successful tenderer to hold a DISP membership. My Procurements will also be reviewed to ensure clear guidance is provided to support Defence officials in incorporating appropriate DISP conditions in a resulting contract.

i. **Contract Management Framework:** Updated to support managers in monitoring DISP membership compliance by their contractors throughout the term of the contract.

7. How the new CRM system is working.

Defence Security launched the DISP Members Portal on 6 December 2023. The DISP Members Portal allows DISP applicants to complete and lodge membership applications (including supporting documentation) online.

The DISP Members Portal has streamlined and modernised the DISP application process for Australian businesses and Defence industry, decreased processing times, supported increased data hygiene and security, and raised confidence in the security of the Defence supply chain.

Since the initial launch in December 2023, the system has remained stable with close to 100% uptime and no major issues affecting service availability. As at November 2024, over 680 new applications have commenced on the Portal with over 340 being submitted for processing.

Defence has continued to develop the Portal to include additional functionality and successfully went live with Capability Release 2 (CR2) on 30 September 2024. This release represented significant progress toward modernising membership processes without compromising security objectives as outlines in the Defence Industry Development Strategy (DIDS).

CR2 delivered initial member self-reporting functionality and allowed DISP members to complete their Annual Security Reports (ASR) and the uplifted Cyber Security Questionnaire (CSQ) on-line. This release also included an on-line Portal for Contract Managers to submit Notification of Engagement Requiring DISP Membership (AE250-2) forms digitally.

Since Go-Live, over 100 ASRs have commenced through the portal, providing confirmation the new services are working smoothly. The portal has delivered clear visibility of compliance including the ability to flag ASRs as overdue and triggering reminders actions to these companies.

The online ASR includes an expanded Cyber Security Questionnaire (CSQ) to align with the Australian Cyber Security Centre (ACSC) Essential 8 (E8) mitigation strategies. To prepare and support DISP members, extensive pre engagement was conducted with members needing to interact with the Portal first, being members with Annual Security Reports (ASR) due from 01 October 2024. A total of 200 members with ASR due in October and November were targeted for additional support, including pre-release virtual Q&A drop in sessions and post-release sessions to obtain feedback and lessons.

An ongoing ASR/CSQ member program will continue to engage with DISP members ahead of their ASR due dates to support them in completing required information and meeting their DISP membership obligations.

Industry feedback from members highlighted concerns around the additional effort needed to complete the up-lifted CSQ. DISB recognised that this release represented a significant uplift in system, process and requirements and have established a dedicated team to support Industry with uplifting their cyber security.

As a result of industry feedback on capacity to absorb change, Final Operating Capability (FOC) will be released in tranches commencing in Q4 2024, delivering incremental enhancements to self-service membership management services across 2025 in collaboration with Industry members.

On achieving FOC, the DMS will transition into a regular cycle of continuous improvement.

8. Audit results of an appropriately sized statistically reliable sample of contracts to demonstrate assurance that those requiring DISP clauses have them included.

Defence audits into procurements are generally concerned with process adherence and do not specifically identify non-compliance with DISP clauses. Whilst there has been significant effort to embed DISP related clauses into Defence contracting, standing offers and panel processes, further work is needed to establish a central contracts data repository to enable DISP auditing of contracts information.

DISP is working with stakeholders across Defence to establish a central register for contracts data. This approach will draw data from disparate systems such as Financial systems and extract data relevant to contracts and DISP clauses, removing the need to share sensitive and non-relevant contract details.

Defence demonstrates the effectiveness of this approach in questions 1, 2 and 3 of this report, providing detail on how the newly developed DISP Contracts and Contract Manager data governance and management approach works in practice. By using required contracts information extracted from across disparate systems, DISP is able to identify contracts that may be in breach of mandatory DISP requirements and will result in further investigation such as an audit. The intent is to continue to build out this approach in collaboration with other Defence initiatives focused on contracts management data.

9. The number of contracts that triggered a non-compliance escalation pathway, and the actions taken, or penalties imposed.

DISP is a membership rather than a contract based program. Companies do not require a contract with Defence to apply for and maintain DISP membership. The DISP approach to non-compliance is most commonly triggered as a result of Deep Dive Audits (DDA) and Ongoing Suitability Assessments (OSA) conducted into members. Other mechanisms for triggering the escalation pathway can include significant security incidents and non-responsiveness of the entity in respect of their membership obligations.

Where DISP members fail to meet the requirements of their membership, Defence employs a scalable approach in responding to non-compliance through its Assurance Criticality and Escalation Framework. The framework is designed to support timely and consistent escalation of security risks and non-compliance. The Framework allows for limitation, downgrade, suspension and or cancellation of DISP memberships for non-compliant members.

A forward work plan has been developed to manage a number of entities through the DISP non-compliance pilot program. It is expected that the initial entities will be progressed through the escalation pathway to resolution in 2025. It is always the goal of the DISP audit and assurance program to work with entities to return to compliance where possible.

10. Advice at that time as to the Department's future approach to DISP audit and assurance.

The DISP is underpinned by an ongoing assurance framework to ensure that members maintain their security maturity. A layered approach is taken to managing assurance through:

- Annual Security Reports: a self-attestation by DISP members of their compliance with their security obligations under the program which is due each year on the anniversary of their membership date.
- Ongoing Suitability Assessments: a desk-top audit
- Deep Dive Audits: in-depth audits that includes site visits to assess compliance

As DISP develops and grows, broader engagement with high-risk enterprise such as Guided Weapons and Explosive Ordinance Group (GWEO), National Shipbuilding and Sustainment Group (NSSG), Australian Submarines Agency (ASA) and AUKUS will inform more tailored assurance models, methods and practices.

DISP provides assurance through a rigorous audit process, that provides assurance over DISP membership including entity handling, transmitting and storing of Defence security classified information and assets, and that of our allies and partners, are compliant with the Defence Security Principles Framework (DSPF), Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM).

Where DISP members fail to meet the requirements of their membership, Defence employs a scalable approach in responding to non-compliance through its Assurance Criticality and Escalation Framework. The framework is designed to support timely and consistent escalation of security risks and non-compliance.

Annex A: DISP Contracts Data Caveats, Data Sources, and Methodology

Caveats

AusTender Data quality (validity, integrity, reliability, timeliness) was assessed as medium to high as per Defence Data Quality process. Categories analysis is a subjective and a qualitative process, which allows for potential margins of errors. For example:

- Some categories have broad nature, due to range of various services included in the scope of contracts. This may result in only part of the scope falling within DISP membership requirement.

Due to volume of data, no validation of actual contractual documents was conducted. The data on AusTender is limited to contracts classified as OFFICIAL.

Contracts classified above OFFICIAL has been identified using Finance data with a publishing reason of either *'Previously blocked as OS'* or *'Not in public interest FOI exempt (Sec appr req)'*.

It should be noted that:

- This information is limited to open outline agreements on the 06/11/2024.
- 1.2% of data provided included a publishing reason.
    - Of 1091 total publishing reasons, 160 of these reasons were for unique outline agreements.

DISP Membership System (DMS) data includes a combination of legacy migrated data and new applications. It is expected that data quality will improve over time as new data is processed. The data does not include historical membership information and excludes membership status of *Withdrawn*, *Terminated* & *Inactive*

Data Sources

AusTender and the DMS. Further data sources will include data such as Enterprise Resource Planning (ERP) once implemented and will be used to continue enhancement of DISP contracts information.

Methodology

Data for Defence contracts published on AusTender between July 2023 to October 2024 were extracted and the *"Categories"* were mapped to the criteria for DISP mandatory membership as per *Defence Security Principles Framework (DSPF), Principle 16 Defence Industry Security Control 16.1.* The matching DISP themes identified indicated either:

- Supply, maintenance, storage or transportation of weapons or explosive ordnance,
- Provision of security services for Defence bases or facilities.

The ABNs on AusTender were compared to the DISP Membership System to identify contracts without current DISP membership or application.

Annex B: DISP Caveats, Contract Manager Data Sources, and Methodology

Caveats

- There is currently no single source of truth established for contract managers, therefore proxy data was used, meaning data that most likely contains contract manager information such as Financial systems. The risk of this approach is that the data may not be 100% accurate. To reduce this risk, the data validation process developed increases confidence in data quality and accuracy.
- The ongoing process may require updates as the data source structures change (i.e. the implementation of ERP).

Data Sources

- For the purposes of demonstrating DISP reporting ability on Contract Manager information, data sources were limited to:
    - Defence Finance Systems: Purchase Order Good Receipts, April 2023-April 2024. Finance Approvers, Current Active outline agreement and/or Purchase Orders with amount remaining.
    - DMS: Customer Relationship System DISP member and applicant data and newly digitised AE250-2 Contract Notification Forms.
    - CASG Major Contracts List.

Methodology

The Contract data validation process developed to increase confidence in data accuracy, completeness, quality and consistency is based on the Defence Data Quality Framework (DDQF).

Proxy data sets were validated using information provided directly to DISP by Entities and Contract Managers in the DMS.

In order to provide 100% confidence in the proxy data used, testing of the whole population would be required, meaning individually confirming with every identified individual if a Contract Manager role was being performed, which was not practical due to the size of the population. Rather, statistical sampling, as a practical and recognised method was used to draw conclusions about a large population to provide a reasonable level of confidence. Proxy data was validated by cross checking with known good data sets within the DMS.

Annex C: DISP Contracts and Contract Manager Data Future Improvements

Initial data DISP Contracts and Contract Manager data governance and management efforts have been focused on developing repeatable methods and processes to identify, integrate and validate data used to better manage compliance of the program and enable data driven DISP assurance activities. DISB has developed a data maturity roadmap to further build on this work as the DMS and dependency data sources mature. Key planned future activities include:

- Embedding DISP flags into key systems enhancements which are underway, such as ERP programs concerned with contract procurement planning, contract execution and contract finance management.
- Establish bi-directional data integration into Defence enterprise contracts data which is currently being developed.

The DISP DMS will continue to enhance and uplift its analytical capabilities in line with improvements to dependency data sources as well as information being provided by DISP Members, Applicants and Contract Managers.

As this occurs, the system will incrementally evolve its analytical capabilities to enable:

- Data driven insights to inform decision making, prioritisation and resource allocation.
- Better informed DISP contract risk management, through reporting on DISP entities and contracts, including changes in circumstances, contract updates, incidents etc.
- Tighten DISP assurance through automated processes utilising modern unstructured data analytics informing targeted audit activities on non-compliant contracts for further review.
- Ensure DISP Contract Manager Training is conducted by reporting on training conducted and contract manager attendance.
- Strengthen supply chain risk modelling by supporting Defence identify connections between entities that form a supply chain, and connections between personnel associated with those entities.