Australian Government
Department of Defence
Defence Security and Vetting Service

Defence Industry Security Office

Audit Fact Sheet

1. What is the Defence Industry Security Office?

The Defence Industry Security Office (DISO) was established within the Defence Security and Vetting Service (DS&VS) to conduct audits and provide assurance that Defence Industry Security Program (DISP) members are meeting their security obligations.

2. What authority does DISO operate under?

The Defence Security Principles Framework (DSPF) Control 16.1, paragraph 29 states that Defence will conduct random and targeted spot checks of DISP members to ensure compliance with DISP minimum security requirements.

DISP members are obliged to participate in these audit activities. Control 16.1, including DISP membership and suitability requirements, can be found here.

3. Why is my company being audited?

We select companies to be audited based on a range of factors. This includes the extent and nature of their interaction with Defence and whether they:

- are involved in Defence build, acquisition and sustainment activities;
- work with sensitive and emerging technology – research and development;
- are listed as a sovereign industrial capability priority – as our focus will be on the Shipbuilding sector; and
- handle sensitive Defence personnel information.

4. What benefit will there be to Defence and industry from these audits?

The key benefit will be an uplift in security. Our audits will review existing security practices and recommend how these deficiencies and highlight additional opportunities to enhance security.

Follow-up audits will assess whether recommendations have achieved their intended outcome. We will share themes arising from our audit program with industry to assist in uplifting overall security practices. This information will be general and anonymised.

5. How are the audits conducted?

Our audits are conducted in line with better practice audit methodologies across the audit lifecycle (planning, fieldwork and reporting).

Member compliance is assessed against the requirements of the DSPF Control 16.1 and DISP suitability matrix (Control 16.1, Annex B) including where applicable, its reference authoritative documents such as the Information Security Manual (ISM) and the Protective Security Policy Framework (PSPF).

6. Why do you use contracted auditors?

Audits are undertaken by ‘blended teams’ – our staff supported by contracted auditors. With the defence industry supply chain expected to grow substantially over the coming years, we need additional assistance.

7. Why do the auditors need to inspect company documents and assets?

To assess your security maturity, our auditors must examine – and on some occasions retain for more detailed analysis – evidence of operations, functions, and processes. We also need you to demonstrate to our cyber auditors how ICT security controls are applied.

DISP members agree that security policies and plans will be made available to Defence upon request when they apply for membership (AE250).

8. How will you protect my information?

We appreciate that information gathered for the purpose of an audit can be potentially sensitive. We will ensure that information you provide is appropriately safeguarded and only used for the purposes of the audit.

Defence have confidentiality provisions in third-party contracts, which are designed to ensure that contract auditors treat your information appropriately; and any information they access through the audits is confidential commercial/proprietary information provided by the Commonwealth under the Deed. It is owned by the Commonwealth and not third parties, and all information is stored on Defence networks.

Additionally, contracted auditors are prepared to sign a Non-Disclosure Agreement if required. If this is required, please provide at least two weeks' notice to allow clearance through legal channels.

9. What happens if areas of my company are found non-conformant?

We want to work with you to uplift security, and we will seek to do this in the first instance. If serious security issues are identified however, Defence's Chief Security Officer is obliged to consider your ongoing suitability for membership. The decision to downgrade, suspend or terminate a company's DISP membership is made by this officer. Our audit reports are also sent to relevant Defence contract managers. These contract managers will determine whether any contractual requirements have not been met, and make a decision on whether any contractual penalties apply.

10. What happens after the audit?

Your CEO (or equivalent senior employee) should formally notify us in writing when you have implemented the audit recommendations. We will then close the audit, though we may conduct a follow-up audit at a later date to review how you have implemented the recommendations.

11. What if I refuse to participate?

We cannot force you to participate in an audit, but if you don't, Defence will not be in a position to determine whether you are meeting your membership obligations, and this could result in suspension, downgrading or termination of your DISP membership. There could also be contractual penalties for not maintaining your membership.

12. What can I expect from DISO?

We will act in an objective and impartial manner free from any conflict of interest, inherent bias or undue external influence or interference. The intent of the audit program is to help uplift security, not to take punitive action – we see ourselves as partners in this process.

13. What does DISO expect from industry?

We ask that you be open and transparent and provide access to documents and assets. We should view each other as trusted partners seeking to improve security.

14. Who does DISO report to?

We report audit program outcomes to the Defence Security Committee on a bi-annual basis. The CSO maintains on-going oversight of program activities and outcomes and we report to the CSO on a monthly basis.

15. What does the audit involve?

Step	Description
Initial notice	We will provide initial notification to industry security officers of audits planned for the following calendar quarter by email. Audits may take place within weeks or months of the initial notification.
Confirm audit dates	A member of our team will be in contact with you to discuss and confirm dates for the audit. Your contact is the audit coordinator and is available to answer any questions you may have about the process.
Formal notification (letter and audit plan)	Once dates are confirmed, a formal notification letter will be provided to the Chief Security Officer or Chief Executive Officer. An audit plan outlining what to expect from the audit will also be provided for planning purposes. The audit plan outlines: • the audit objective and scope; • what to expect regarding fieldwork; • the audit team; and • the reporting steps.
Fieldwork	Fieldwork comprises of a blended team of Defence and contracted audit staff (including cyber) on site for 3-5 days interviewing relevant security officers, sighting documents, and providing an initial assessment on the last day of the field work. The number of fieldwork days will depend on the scope of the audit.
Initial findings discussion	A verbal briefing will be held following our site visit to discuss our initial findings with you and give you an opportunity to provide any clarifying information before we develop the draft audit report.
Draft audit report	A draft audit report will be prepared outlining our findings, maturity rating, and any recommendations we have identified to further enhance security practices. The report will be provided to you for comment and, as required, completion of an action plan.
Action plan (if applicable)	Your action plan should outline how you plan to implement the recommendations, the responsible staff, and timeframes for completion. We will include this plan in the final audit report.
Final audit report	The final audit report is the formal record of the audit – outlining our findings, the maturity rating and recommendations. The report will be provided to the First Assistant Secretary Security & Vetting Services (Defence Chief Security Officer), relevant contract managers, and other key stakeholders. A copy of the final audit report will be provided to you for your records.
Audit closure	After you have implemented the audit recommendations, your CEO (or equivalent senior employee) should formally notify us in writing. This letter should include a table listing the recommendations and details of how you have implemented each one. The audit is formally closed upon our acceptance of this letter, though we may conduct a follow-up audit at a later date to review your implementation of the recommendations.

16. How can I contact DISO?

You will receive the contact details of your audit coordinator when we issue the formal audit notification. Queries can be directed to DISO.info@defence.gov.au.