Australian Government
Department of Defence

Ai GROUP | DEFENCE COUNCIL

Australian Industry Group
and Department of Defence

WORKING **SECURELY** WITH **DEFENCE**

A guide to the Defence Industry Security Program membership

February 2021

WORKING SECURELY WITH DEFENCE

A guide to Defence Industry Security Program membership

This Guide has been developed by the Security Working Group of the Australian Industry Group (Ai Group) Defence Council in cooperation with the Department of Defence. It is designed to help any business or organisation that would like to work with or expand their engagement with Defence and Defence industry.

We would like to express our gratitude to the members of the Ai Group Defence Council Security Working Group, as well as our other industry, Government and Defence partners, who have shared their expertise and worked in the spirit of collaboration to help us complete this Guide. As this is the first edition of the Guide, it will be updated from time to time. Please note that the content is subject to change.

SPECIAL ACKNOWLEDGEMENTS:

ASC Pty Ltd

Australian Industry & Defence Network

BAE Systems Australia

IBM Security

Thales Australia

Thomas Global Systems


672D

Contents

Foreword

The Morrison Government's commitment to invest $270 billion over a decade to modernise Australia's Defence capabilities is creating significant opportunities for Australian industry.

Forming partnerships with industry will be critical to capitalising on this investment and enabling us – together – to support the men and women of the Australian Defence Force.

Defence and industry have a long history of working hand-in-hand to build Australia's sovereign Defence capabilities. All Defence businesses, be they small, medium or large, have a critical role to play.

More can – and indeed will – be done to leverage the expertise of our very capable Australian businesses, giving us the chance to grasp the opportunities and provide industry with the right support to promote greater access to Defence work.

In April 2019, the Morrison Government reformed its Defence Industry Security Program (DISP) to make it easier for industry to do business with Defence.

Importantly, DISP members can now easily access security information and assistance to ready themselves for working in Defence. These reforms have been very well received by industry and open the door for a larger and more diverse range of businesses to build partnerships with Defence.

The timing for these reforms is critical. Security threats to our defence industry highlights the importance of Australian businesses being provided with the most up-to-date and reliable tools to protect Australia's sensitive and classified information, as well as industry's intellectual property.

To build on the reformed DISP, Defence and industry have worked together, through the Australian Industry Group (Ai Group) Defence Council, to develop *Working securely with Defence: A Guide to the Defence Industry Security Program*.

This Guide includes industry-led advice and covers major aspects of defence-related security. It is designed to help more businesses get involved in working with Defence by joining the DISP, as well as strengthening the security and competitiveness of the industry.

It complements the Morrison Government's 'five pillars' approach to supporting Australian businesses by improving the way Defence communicates and does business with industry in relation to its security obligations.

The development of this Guide has been a genuine partnership, drawing on deep expertise and connections across Government, Defence, Australian defence industry members and industry associations. We would like to thank all involved for their time and contributions.

The Hon Melissa Price MP
Minister for Defence Industry

Innes Willox
Chief Executive
Australian Industry Group

Introduction

Welcome to Working Securely with Defence: A Guide to Defence Industry Security Program (DISP) Membership.

There are sound security and commercial reasons why you might consider joining the DISP if you are currently in the Defence industry or wish to work with Defence in the future.

Defence encourages all organisations interested in working with Defence to consider applying for DISP membership and, in some cases, it is mandatory to join the program if you are doing sensitive or classified work at a non-Defence facility.

DISP supplier companies include many Australian and multinational industry leaders. As a member of the DISP, you will have access to best practice information and advice, as well as the opportunity to enhance your security practices.

The purpose of this Guide is to:

- provide the pathway for your business to become eligible for classified and sensitive Defence work through participation in the DISP;
- provide practical guidance, tools and expert advice to help protect Australian organisations from a range of security threats;
- help build the competitiveness and security resilience of the Defence industry sector through good security practices; and
- assure international investors and partners of industry's commitment to Defence security.

While this Guide is primarily designed to help you navigate the DISP, it is important to note that many small to medium enterprises will be working in a supply chain with larger Defence industry companies. It will therefore be critical to understand the specific security requirements of those larger companies, which will complement the DISP processes. We provide more information on working with larger companies in Chapter 9.

This Guide has been designed as a companion document to the DISP website (https://www1.defence.gov.au/security/industry) and should be read in conjunction with all information provided by Defence. The DISP website will be regularly updated to reflect any changes to policy and regulation and is therefore the primary source of information.


850J

Chapter 1: Understanding the defence security environment

On 1 July 2020, the Prime Minister announced the 2020 Defence Strategic Update and the 2020 Force Structure Plan. These documents outline a revision to Australia's strategy in responding to evolving challenges and destabilising forces identified in the 2016 Defence White Paper. The realisation of these challenges has been accelerated by a number of factors, including the global coronavirus pandemic. Australia's strategic environment has deteriorated quicker than anticipated. Australia is operating in a period of global transition, seeking to uphold the maintenance of rules based order. To do this, the updates call on Defence to shape Australia's strategic environment, deter actions against Australia's interests and respond with credible military force.

The 2020 Force Structure Plan refers to credible military force in five domains, being the:

1. Information and cyber domain;
2. Maritime domain;
3. Air domain;
4. Space domain; and
5. Land domain.

The expansion of Australia's military capability beyond the tri-service environment, into five domains, represents a significant shift in Australia's military structure. The update demonstrates Australia's move toward military modernisation that is prepared to counter contemporary threats and respond with credible military force. These will enable: competition; increased potency and military endurance; response to grey zone tactics; decisive action in deterrence of threats against Australian interests; values based approach; and sovereign capability.

Australia faces a range of sophisticated and persistent espionage and foreign interference threats from hostile foreign intelligence services. Many of the adversaries targeting Australia are highly capable and have the intent and persistence to cause significant harm to our nation's security, information, assets and people.

Defence and associated industry are prime targets for hostile foreign intelligence services. We have already experienced alarming breaches and attempted breaches of Defence industry organisations that could impact our nation's safety and future prosperity.

1. What are the major threats to the Defence industry?

The current environment includes threats from a range of sources, but not limited to:

Foreign government/state sponsored attacks

The intelligence services of foreign governments present an enduring and serious espionage and foreign interference threat to Australia and Australian Defence industry. State-sponsored espionage operations, particularly in the cyber realm, are often extremely well resourced and sophisticated, using high level and complex tools and capabilities. It is important to note, however, that foreign intelligence services will sometimes outsource their work to contract hackers to increase the deniability of their operations. Such contracted operations may employ much less sophisticated tools, increasing the range of challenges for network security staff.

Cybercrime

Australia is a very attractive target for cybercrime given our prosperity, use of online facilities, government services and social media. Cybercrime can have devastating effects on businesses, including but is not

limited to: theft of intellectual property, sabotage, bribery and loss of competitive advantage through insider knowledge. All Australian businesses are at risk from cyber criminals, however there are additional national security considerations in play for businesses supporting Defence.

The Government has stated that cyber security incidents cost Australian businesses up to $29 billion each year, with almost one in three Australian adults impacted by cybercrime. Experts recognise that cyber attacks are not a matter of 'if' but 'when', and these attacks are continually growing and evolving. The intensity and volume of attacks makes us all vulnerable.

Examples of cybercrime include ransomware and credential harvesting malware and further details can be found at the Australian Cyber Security Centre (ACSC) website: https://www.cyber.gov.au.

Human error and insider threats

Good security is as much about shaping human behaviour as it is about putting in place technical network defences and controls. Whether through error or intent, people can be one of our biggest vulnerabilities in terms of security incidents, cyber attacks and data breaches. Anyone who has access to your IT systems or sensitive information, whether they are employees, subcontractors, legal advisers, accountants, consultants or vendors can make your system vulnerable to cyber attacks and other security breaches.

The insider threat is also a growing problem for many businesses and refers to unauthorised access, use or disclosure of privileged information, techniques, technology, assets or premises by an individual with legitimate or indirect access, which may cause harm. Trusted insiders can intentionally or unknowingly assist external parties in conducting activities against the organisation they work for, or can commit malicious acts for self-interest. Examples of such threats include disclosure of sensitive information, sabotage, theft, financial fraud and enabling unauthorised access to sensitive or classified material. According to the Ponemon Institute, the average cost of insider threats annually is USD $11.45 million in 2020.[1]

CASE STUDY

Internal criminal activities and security risk

The IT Manager of an SME company noticed that for a number of weeks the data usage was spiking at lunch time, a period when there was normally a lull. It turned out that a number of staff were playing a multiplayer role-playing game on the system. Unauthorised software was not permissible on the work systems unless it had been approved through relevant IT channels. The software was removed from the system and staff involved counselled.

At the same time, a staff member reported receiving an offer of cheap CDs and DVDs from another staff member. The matter was reported to ensure the promotion was not linked to video pirating in any way. The matter was referred to corporate security and the official investigation revealed the following:

[1] Ponemon Institute, 2020 Cost of Insider Threats Global Report (January 2020).

- The material was pirated and of substantial volume;
- The perpetrator had set up deals to import the material and was using the company network to promote sales;
- The perpetrator had taken pictures of themselves in classified work areas and with military equipment to promote their importance to a person overseas involved in the supply operation;
- The role-playing game was one of the pirated products; and
- A substantial number of staff had purchased CDs and DVDs with people in the company without questioning the source.

The perpetrator was dismissed for multiple breaches and Defence advised. All staff in receipt of the material were counselled and required to surrender the goods.

Security advised the relevant copyright and anti-pirating authorities, who supported the company's actions to remedy the situation.

What can you do to mitigate this situation?

- Monitor data usage and identify and investigate anomalies;
- Encourage staff reporting of inappropriate emails and suspicious offers; and
- Ensure that policy, processes, training and response requirements are clear and up to date.

Risks in the global and local supply chain

The risks inherent in your supply chain, which includes the materials for supply of services and production of goods, are easily overlooked but they can be significant. Hostile foreign intelligence services are alert to possibilities offered by what could be a series of security risks in your supply chain.

You may suffer material loss and degradation or poor-quality substitution if the physical aspects of your supply chain are not secured. Intellectual property can also be compromised through the supply chain. While an organisation may have strong cyber security within its business, it may still be vulnerable to cyber attacks and security breaches through its supply chain network of third parties, vendors and other partners.

Sharing and aggregation of sensitive information between organisations within a trusted network via cloud services may be of interest to a cyber attacker. This might include, for example, your legal service providers or accountants. Referred to as secondary targeting, the cyber attacker will explore alternative routes to gain access to the same information from another organisation within the trusted network.

2. The Defence security environment, legislation and reporting

Building strong security resilience in the current threat environment requires government and industry to deploy a range of tools and measures. As part of this, the Australian Government has introduced additional legislation and increased regulation levels and has released key policy documents to help manage security risks. It is important that you understand the changing regulatory environment as well as the reporting requirements, which may affect your business both inside and outside the Defence security environment.

Important legislation, regulation and policies that guide Defence industry security include the following:[2]

1. **The Australian Government Protective Security Policy Framework (PSPF):**
   - PSPF sets out the revised security policy for Government entities, including governance, information, personnel and physical security.
   - The principles and requirements within the PSPF flow down into the requirements for the DISP.

2. **The Defence Security Principles Framework (DSPF):[3]**
   - The DSPF provides principles, controls and instructions to support Defence personnel, contractors, consultants and outsourced service providers, to manage security risks.

3. **The Australian Government Information Security Manual (ISM):**
   - The Australian Cyber Security Centre (ACSC) within the Australian Signals Directorate (ASD) produces the Australian Government ISM.
   - The purpose of the ISM is to outline a cyber security framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats.

4. **Espionage and Foreign Interference Act and the Criminal Code Act:**
   - The *Criminal Code Act 1995* (Cth) was amended on 29 June 2018, as a result of the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) (EFI Act).
   - The EFI Act amendments modernise and strengthen a range of espionage offences and introduce a number of new foreign interference laws, as well as a new aggravated offence for providing false or misleading information during a security clearance process.

5. **Privacy Act 1988 (Cth):**
   - This legislation obligates industry to protect the privacy of individuals.
   - It includes the Notifiable Data Breach (NDB) obligations.

6. **Customs Act 1901 (Cth):**
   - This legislation is the basis for controls on the export of tangible Defence and strategic dual-use goods and technologies.
   - The administering agency for the Customs Act is the Australian Border Force (ABF).

7. **Defence and Strategic Goods List (DSGL):**
   - Controls are executed through the Customs (Prohibited Exports) Regulations 1958, Regulation 13E.
   - This Regulation allows for permission to export regulated goods and technology listed in the DSGL (updated regularly).
   - Defence Export Controls (DEC) is responsible for issuing export permits and licences.

8. **Australian Human Rights Commission Act 1986 (Cth):**
   - Provides for the Australian Human Rights Commission with the authority to investigate any complaint of unlawful discrimination.

---

[2] Refer to Annex A for a more detailed review and key website links.
[3] A DPN/DOSD July 2020 version of the DSPF can be accessed by DISP members. Non-DISP members can access the public version here: https://www1.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL.pdf. This Guide was developed based upon the following version: https://www.defence.gov.au/DSVS/_Master/resources/DSPF-Unclass-Version.pdf.

In terms of overseas regulations, you might also note the following:

9. **European Union's General Data Protection Regulation (EU GDPR):**
    - Applies if you are an entity which employs EU citizens (e.g. overseas staff or subcontractors) in your Defence work – you will be automatically obligated to comply with the EU GDPR.

10. **Defense Federal Acquisition Regulation Supplement (DFARS) and Federal Acquisition Regulation (FAR):**
    - These US-based regulations are a requirement if your entity in Australia exports products or services procured by the US Department of Defense or your entity operates in the US Defense supply chain.

11. **International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR):**
    - Many Australian exporters in the Defence industry manage controlled technology that may be subject to US export controls, which have extraterritorial reach. This includes the ITAR and EAR.

3. Who is involved in Defence and Defence industry security?

There is a range of Government, Defence and other organisations that have important roles and responsibilities in relation to Defence and Defence industry security. It is useful to familiarise yourself with these organisations and understand what they do, as well as key contact information:

- **The Defence Security and Vetting Service (DS&VS)** in the Department of Defence is responsible for leading Defence's protective security initiatives including the Australian Government Security Vetting Agency (AGSVA) and the DSPF. Importantly, DS&VS also operate the DISP program and will be your key link into membership and ongoing obligations for the program. Website: https://www1.defence.gov.au/security.

- **The Defence Industry Security Office (DISO)** is an organisation within DS&VS and provides independent assurance that DISP members are meeting their membership obligations.

- **The Australian Government Security Vetting Agency (AGSVA)** is an organisation within DS&VS and is the central personnel vetting agency for the Australian Government and conducts security clearance assessments for Federal, State and Territory agencies and for employees in the Defence industry who are required to have Australian Government Security Clearances. Website: https://www1.defence.gov.au/security/clearances.

- **The Chief Information Office Group (CIOG)** in the Department of Defence is responsible for leading the design, delivery and operation of the information, computing and communications infrastructure to support military operations. The CIOG has important responsibilities relating to Defence industry security for information and communications technology (ICT) systems. Website: https://www1.defence.gov.au/about/chief-information-officer-group.

- **The Australian Cyber Security Centre (ACSC)** within the ASD is responsible for monitoring cyber threats in Australia and providing cyber security advice to individuals and businesses. Website: https://www.cyber.gov.au.

- **The Centre for Defence Industry Capability (CDIC)** within the Department of Industry, Science, Energy and Resources is responsible for supporting Australian small and medium-sized businesses to enter or work in the Defence industry. The CDIC provides a range of advice,

business services and grants programs that could help with your security needs. See more information on grants in Chapter 2. Website: https://www.business.gov.au/CDIC.

Australian Security Intelligence Organisation (ASIO) support

A further government resource to aid Australian companies in understanding the current security and intelligence risk is ASIO's Outreach team, elements of which were formerly known as the Business Government Liaison Unit. ASIO provides a very useful subscriber-based website offering which can be found at https://www.outreach.asio.gov.au/.

In addition to its website offering, ASIO is able to provide information via a number of means including ASIO-hosted briefings, face-to-face engagement and participation in joint government and industry forums. All these mechanisms are aimed at providing risk management decision-makers within government and industry with the most current security intelligence and protective security advice to assist them to:

- recognise and respond to national security threats;
- develop appropriate risk mitigation strategies; and
- provide informed briefings to executives and staff.

The ASIO Outreach secure website operates on a free subscription basis and contains intelligence-backed reporting on the domestic and international security environment. This reporting is drawn from the full range of ASIO's information holdings and expertise (including the multi-agency National Threat Assessment Centre, ASIO's protective security area (T4) and the Counter-Espionage and Interference Division) and some foreign intelligence partner agency reports.

4. A security-in-depth approach – layering your defences

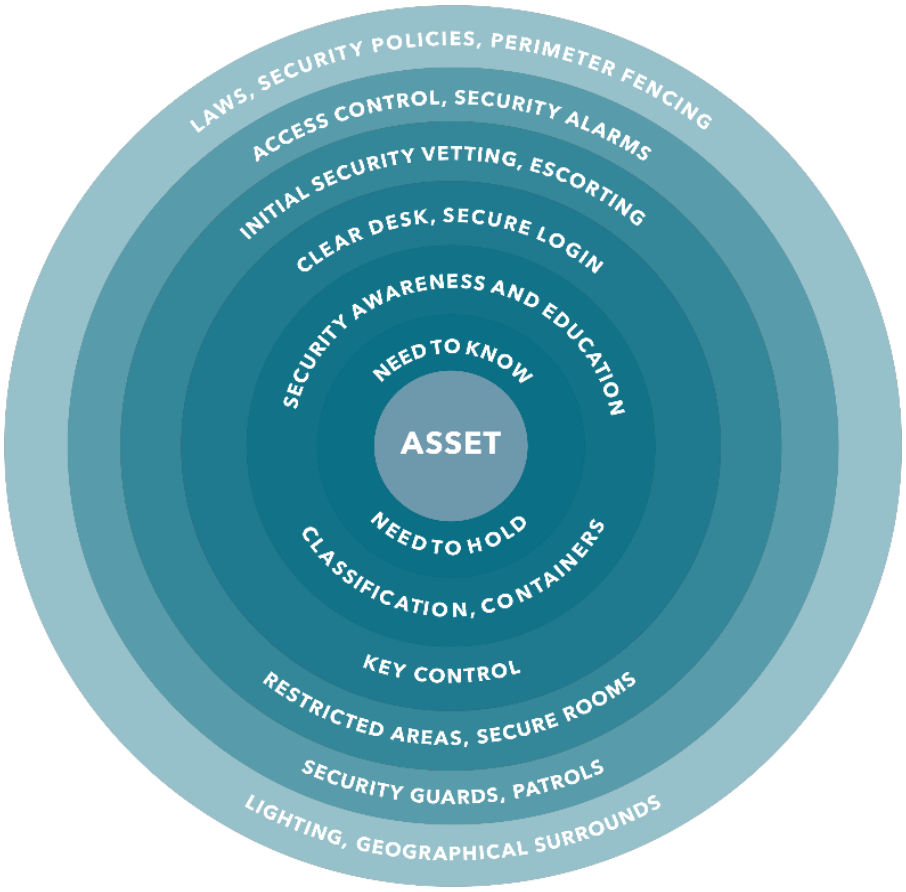
Australian businesses are becoming more aware of security risks, particularly in the Defence industry which has recently experienced several high-profile attacks. These kinds of attacks can have serious impacts on Defence capability, the financial viability of businesses, as well as Australia's competitive position in global markets.

Defence and industry have learned from these experiences, however, threats and associated risks are constantly evolving so Defence and industry must too.

Protecting against cybercrime, espionage, unauthorised access and data breaches is becoming increasingly challenging for governments and businesses of all sizes. However, there are many things you can do to raise your levels of security protection and minimise your risks.

Experts recognise that protective security requirements are multi-layered and interdependent. For example, threats can be external or internal involving personnel with access to OFFICIAL and classified information or assets. Threats can be cyber related if the adversary uses technological means to gain access to an environment that contains OFFICIAL and classified information or assets.

It is an important reminder that security controls should not be considered in isolation from each other. This multilayered approach to security is referred to as Security-in-Depth (see figure below). As explained further in this Guide, becoming part of the DISP will help ensure you are playing your part in a Security-in-Depth approach.



Source: DISP Security Awareness Training

Chapter 2: About the Defence Industry Security Program

1. An introduction to the Defence Industry Security Program

The revised Defence Industry Security Program (DISP) was launched on 9 April 2019 to meet the requirements of a modern Defence organisation.

The reformed DISP represents a fundamental change in approach to industry security, providing an effective way for Defence and industry to work together to protect sensitive, OFFICIAL and classified Defence information and assets, as well as industry's intellectual property.

The DISP:

- is a membership-based program for industry that sets minimum security requirements;
- helps secure Defence capability, Defence industry and the supply chain;
- requires its members to comply with Defence's protective security policies, practices and procedures;
- uses a tiered level of membership tailored to individual business needs;
- includes a system of reviews to ensure continued compliance; and
- enhances Defence's ability to monitor and mitigate security risks.

The DISP is managed by the Defence Security and Vetting Service (DS&VS) within the Department of Defence and involves:

- an online website to help industry obtain entry and manage their membership: https://www1.defence.gov.au/security/industry; and
- support and services provided by Defence personnel to help you navigate membership, as well as access training, support, reporting and assurance services.

Additional help and support is available through: disp.info@defence.gov.au or 1800DEFENCE.

NOTE

Even if you are a member of the previous DISP program, you must transfer membership to the new DISP. Existing members have until 9 April 2021 to transition to the new DISP before the old program closes. During the application process Defence will consolidate multiple memberships under a single entity membership.

Existing DISP members are unable to enter into a new contract, or amend an existing contract, until they successfully transition into the new program.

The above only applies to new or amended contracts requiring DISP membership. As such, a company could enter into a new contract that does not require DISP membership.

2. What are the benefits of DISP membership?

The Australian Government is investing $270 billion over the next decade in Defence capability and we are building a world class Defence industry. The DISP offers substantial benefits to Defence and industry in terms of streamlining security services and protecting Defence information and assets, as well as industry's intellectual property.

In some instances, DISP membership is mandated by the nature of work delivered to Defence or as a result of a Defence business requirement specified in a contract. For some entities, DISP membership will not be required, however membership is strongly encouraged to ensure they meet minimum security requirements to engage with Defence at a later stage, or as a demonstration of sound security practice even when handling OFFICIAL information.

DISP benefits to industry include:

- Improved security operating environment for your business as security practices are strengthened.
- Access to Defence security services that will enable you to be 'Defence-ready' when delivering contracts and tenders.
- Ability to sponsor your own security clearances (not available for Entry Level membership).
- Greater access to international contracts as you may be able to have your security clearances recognised by international partners.
- Security training and materials, including cyber training.
- Advice and analysis on the latest security trends and threats to better inform your security planning and practices.

In some cases, a membership profile above Entry Level can take time to process due to certification and accreditation for physical, and ICT and cyber security. To avoid delay, it is recommended that companies apply at a minimum for Entry Level membership across all four security membership categories. Once a member of the DISP, industry members would then have the option to upgrade to a higher level of membership if necessary.

DISP membership may also be beneficial if you are seeking to enter a supply chain and work with one of the larger Defence companies. Most larger companies have their own supply chain security requirements and being a DISP member can be an important step to lay out your security credentials when looking to work in a supply chain. More information on working within supply chains is in Chapter 9.

NOTE

DISP membership will continue after a contract ceases, until a member withdraws, or the DISP member is found not to be meeting the suitability criteria for their chosen level of DISP membership.

3. What are the levels of DISP membership and associated security classifications?

The reformed DISP has tiered levels of membership that can be tailored to suit your organisation's needs.

A DISP member may hold different levels for different categories of security. For example, a DISP member may be Entry Level for ICT and cyber security, but Level 1 for governance, personnel and physical security. Note that governance must be equivalent to the highest level of accreditation sought for the other categories.

The DISP has four membership levels within each membership category that align with access to the level of information associated with security classifications (OFFICIAL, OFFICIAL: Sensitive, PROTECTED, SECRET and TOP SECRET):

	Governance	Personnel Security	Physical Security	ICT and Cyber Security
Entry Level	OFFICIAL / OFFICIAL: Sensitive	OFFICIAL / OFFICIAL: Sensitive	OFFICIAL / OFFICIAL: Sensitive	OFFICIAL / OFFICIAL: Sensitive
Level 1	PROTECTED	PROTECTED	PROTECTED	PROTECTED
Level 2	SECRET	SECRET	SECRET	SECRET
Level 3	TOP SECRET	TOP SECRET	TOP SECRET	TOP SECRET

3.1 What are the security classifications used in DISP?

The new Australian Government security classification system commenced from 1 October 2018, with full implementation required by 1 October 2020. Below is a summary of the changes.[4]

THEN	→	NOW
TOP SECRET	Security classifications	TOP SECRET
SECRET		SECRET
CONFIDENTIAL		N/A
PROTECTED		PROTECTED
Sensitive: Cabinet	DLM → Caveat	CABINET (Caveats can only be applied to security classified information, i.e. PROTECTED or above)
Sensitive	DLM → Information management marker	Apply classification or OFFICIAL: Sensitive and optional information management markers: • Legislative secrecy • Personal privacy • Legal privilege
Sensitive: Personal		
Sensitive: Legal		
For Official Use Only	DLM → DLM	OFFICIAL: Sensitive
UNCLASSIFIED	Non-classification markings	OFFICIAL
UNOFFICIAL		UNOFFICIAL

NOTE

- Documents that were marked RESTRICTED should be handled in accordance with PROTECTED marking.
- There may also be caveats on documents that have certain controls such as Australian Eyes Only (AUSTEO).

More information on how Defence classifies information can be found at Annex B.

[4] For further information about the transition from the old classification, see: https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx; https://www.protectivesecurity.gov.au/sites/default/files/PSPF-fact-sheet-classification-reforms.pdf.

3.2 What is the terminology used for personnel clearances?

The DISP also requires an understanding of the terms used to describe personnel clearances:

- **Baseline clearance** – this is the minimum clearance required to work in Defence. It allows access to classified information and resources up to and including PROTECTED level. It requires at least a five year background check.
- **Negative Vetting 1 (NV1)** – this clearance level allows access to classified information and resources up to and including SECRET. It requires a 10 year background check.
- **Negative Vetting 2 (NV2)** – this clearance level allows access to classified information and resources up to and including TOP SECRET. It requires a 10 year background check.
- **Positive Vetting (PV)** – this clearance level allows access to all classified information and resources at all classification levels. It requires a whole of life background check and will also require you to undergo a psychological assessment.

More information on personnel security is in Chapter 5.

4. Who is eligible for DISP membership?

Any Australian business can apply for DISP membership.

To successfully become a DISP member you will need to meet the eligibility and suitability requirements outlined in Control 16.1 DISP of the Defence Security Principles Framework (DSPF).

Control 16.1 of the DSPF relates specifically to the DISP. It provides principles, controls and instructions to support Defence industry to understand and manage security risks when engaging with Defence.

See website for more information: https://www1.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL.pdf.

5. What are the expected costs required for DISP membership?

Although there is no direct cost associated with DISP membership, there may be costs associated with implementing and maintaining security measures to meet initial and ongoing DISP requirements. These might include, for example, facility certification and accreditation, personnel security clearances, and physical security measures.

Organisations should consider these costs in relation to the level of DISP membership required prior to lodging their DISP membership application.

Some businesses may find their existing security practices are well advanced for membership without additional costs and others may need to address a gap in requirements. Businesses should consider these costs in relation to the level of DISP membership required prior to lodging their DISP membership application.

Achieving an adequate level of security means more than complying with regulations or implementing commonly accepted best practices. Each organisation must determine its own definition of 'adequate'. The range of actions an organisation must take to reduce security risk to an acceptable level depends on the value at risk and the consequences if the risk is realised. Accordingly, good security practices should be implemented as a prudent business strategy, whether or not DISP membership is achieved, as these also contribute to the continued protection of business capability.

It is recommended businesses review the options available for grants through CDIC to assist with physical, ICT and cyber security infrastructure and consulting costs. See the next section for further information.

5.1 What questions should I ask in determining the expected DISP costs?

You might consider the following questions in determining possible costs for DISP requirements. Your answers will aid an understanding of your security risks and requirements:

- What is the value in your business that you must protect? Value can be expressed as a product or service, a process, your reputation and/or relationships.
- To sustain this value, what assets must be protected? Why must they be protected? What happens if they are not protected? Assets may include information, technology (hardware, software and systems), facilities, and people.
- What potential adverse conditions and consequences must be prevented and managed? At what cost? How much disruption can the business bear before you must take action?
- How do you determine and effectively manage residual risk (i.e. the risk remaining after mitigation actions are taken)?
- How do these answers inform an effective, implementable, enforceable security strategy and plan to achieve the required DISP level?

5.2 What types of costs do I need to consider for DISP membership?

The following lists examples for calculating what it might cost to join the DISP. It is meant to provide a level of understanding of the effort and potential costs involved. These costs are a rough guide only and should not be taken as definitive advice. Any actual costs will depend on a range of variables, including your existing level of security and the level of DISP membership being applied for.

POTENTIAL COSTS TO CONSIDER FOR DISP MEMBERSHIP INCLUDE THE FOLLOWING:

Chief Security Officer/Security Officer training. Even in a small company, a single Chief Security Officer/Security Officer will need to undertake the required training course which runs for one day. This is an "opportunity cost" for any staff to attend plus travel or accommodation costs involved. The course is operated by Defence with no fee to the participants and is not required at Entry Level.

Development of DISP plans and procedures. Some Australian small and medium-sized businesses have reported effort of several weeks for their Security Officer and senior staff to help meet the Entry Level requirements of the DISP. Individual companies will need to calculate the cost – based on an example $500 per day for 15 working days, that is a minimum of $7,500 or a combined effort of a minimum of $20,000 for 40 days. The level of effort is driven by the level of DISP membership sought and the company's existing preparedness.

This effort also includes development of a Security Practices and Procedures, a Security Register, staff attendance at awareness training, establishing staff procedures in employee handbooks and insider threat

processes. Templates for Security Practices and Procedures and the Security Register are available from DS&VS. Having staff with security knowledge, skills and qualifications also reduces the time to complete documents which meet Defence requirements.

Personnel security clearances. Industry is required to pay the cost of security clearances for business personnel. These costs are: $637.67 for a baseline clearance; $1,327.27 for Negative Vetting 1; $2,267.54 for Negative Vetting 2; and $10,713.95 for Positive Vetting. More information on security clearances is in Chapter 5.

Physical perimeter and internal security measures. These costs will depend both on the level of physical security accreditation needed and the preparedness of the company. Costs for this requirement could vary significantly depending on the needs of your business.

ICT and associated costs. Businesses should consider licensing for appropriate antivirus and other protective software. These measures are generally a prudent business undertaking whether or not your business applies for DISP membership. Costs can vary significantly depending on the needs of your business.

Security consultancy costs. Some businesses may wish to consider the cost of hiring a consultant to assist in developing DISP security requirements. Typically consultants can cost in the order of $1,000 - $2000 per day. More information on selecting a consultant is discussed below.

From the above, current experience indicates a cost to a smaller company, without prior DISP experience, might be in the order of $10,000 or more to achieve Level 1 DISP membership depending on the size and nature of your company.

While this might be seen as cost prohibitive to some, it should be remembered that a significant amount of this effort is prudent business practice and preparation regardless of DISP membership. In addition, Defence provides templates and advice to assist the process and minimise costs.

To minimise costs associated with joining DISP you might consider:

- using the available templates on the DISP website and in this Guide; and
- applying for a relevant grant to assist with these costs – more information on available grants is discussed below.

Available grants

Businesses may be eligible for services and grants to help them prepare to work with Defence, including:

- **CDIC – Advisory and Facilitation Services.** Provides eligible small and medium-sized businesses in the Defence sector with advisory and facilitation services in areas such as business management, innovation collaboration, export activities and supply chain facilitation to improve their business capabilities, extend networks and help them take advantage of development opportunities within the Defence sector. Website: https://www.business.gov.au/grants-and-programs/defence-industry-advisory-and-facilitation-services.
- **CDIC – Capability Improvement Grants.** Provides those who have received a CDIC advisory or facilitation services report with grants of between $2,500 to $150,000 to reimburse up to half of the cost of engaging a consultant or expert to implement the recommendations in the report that

meet the Capability Improvement Grants eligibility criteria. Website: https://www.business.gov.au/grants-and-programs/capability-improvement-grants.

- **Empowering Business to Go Digital – Department of Industry, Science, Energy and Resources**. The Empowering Business to Go Digital program will provide a single grant of up to $3 million to support the establishment of a non-government organisation to build and enhance small business digital capability and to address issues raised in the Small Business Digital Taskforce report. The program will run from 2019-20 to 2021-22. www.business.gov.au provides information and advice to customers via a range of channels including phone (13 28 46), email and web chat. You may receive information related to companies developing services under this grant. Website: https://www.business.gov.au/Grants-and-Programs/Empowering-Business-to-go-Digital.

- **Sovereign Industrial Capability Priority Grants.** Helps Australian small and medium-sized businesses to invest in projects that build capabilities aligned with Defence's stated Sovereign Industrial Capability Priorities. The Defence Industrial Capability Plan identifies an initial list of Sovereign Industrial Capability Priorities. Defence will review the priorities periodically and updates will be published on Defence's website. Of note is that project activities can include: buying, leasing, constructing, installing or commissioning of capital equipment including specialist software to enhance cyber security; and workforce training and accreditation. Further information on the Sovereign Industrial Capability Priorities is available here: https://www1.defence.gov.au/business-industry/capability-plans/sovereign-industrial-capability-priorities.

- **Entrepreneurs' Programme – Business Growth Grants – Department of Industry, Science, Energy and Resources**. If you have received an Entrepreneurs' Programme Business Management service and your business adviser/facilitator recommends specific business improvement activities to increase your business's capability to trade in Australian markets and/or markets in other countries, you can apply for a business growth grant. Business growth grants are small grants to engage external expertise to help you implement the recommendations in your plan. If your plan advises that you require DISP to be competitive and effective in your market then assistance is clearly an option. Website: https://www.business.gov.au/Grants-and-Programs/Entrepreneurs-Programme.

INDUSTRY TIP

Although it is not a requirement, you may wish to engage a security consultant to assist your business with self-assessment for your DISP application, and you will need to account for costs associated with this.

The following are questions for you to consider when deciding on a consultant:

- **Does the consultant hold Negative Vetting Level 1 (NV1) clearance or higher to assess and discuss your company's specific gaps in regard to DISP requirements?**

- **Does the consultant have examples of delivering for Australian Government information and communications technology (ICT) policy – specifically in relation to the following standards and requirements?**

- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 and 27002
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 (US International Traffic in Arms Regulations (ITAR) requirement)
- UK Defence Standard (Def Stan) 05-138
- ASD Essential 8
- Information Security Registered Assessors Program (IRAP) Network hardening certification
- Office of the Australian Information Commissioner (OAIC) Notifiable Data Breach (NDB)

- **Can the consultant provide you with guidance on how to protect against the following incidents?**
  - Insider threats
  - Data loss
  - ICT vulnerability management
  - Cyber security threat management
  - Cyber security incident response planning

- **Is the consultant a member of an international standards association for cyber security and hold current certifications?**
  - IRAP Assessor
  - Examples: Information Systems Audit and Control Association (ISACA) certification (Certified Information Systems Security Professional (CISSP)/Cyber Security Nexus™ Practitioner (CSX-P), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified in the Governance of Enterprise IT (CGEIT) or Certified Information Systems Auditor (CISA))
  - Other information technology (IT) Governance certifications include Control Objectives for Information and Related Technology (COBIT), and ISO/IEC 27001 and 27002

- **Can the consultant provide guidance and certification for physical security requirements when supporting Defence security systems?** For example:
  - Australian Security Intelligence Organisation (ASIO) T4 physical security requirements
  - Catalogue of Security Construction Equipment Committee (SCEC) approved hardware & equipment: https://www.scec.gov.au/
  - SCEC certification – more information regarding SCEC Security Zone Consultants is available from T4 Protective Security: https://www.scec.gov.au/consultants-and-locksmiths
  - Is the security consultant licensed for the activities they are being engaged for? Each State and Territory has legislation which provides licensing requirements for the security industry and most States and Territories require consultants to be licensed and have a publicly available register

- **Does the consultant have technical or university qualifications in security practice or security risk management?**

- **Is the security consultant a member of the Australian Security Industry Association Ltd (ASIAL) professional recognition program, or equivalent overseas qualification such as the American Society for Industrial Security (ASIS) International Certified Protection Professional (CPP), Physical Security Professional (PSP) and Chartered Security Professional UK (CSyP)?**

6. What are the timeframes for processing DISP memberships?

Timeframes for processing DISP membership vary based on the required level of membership, current level of security maturity and requirements and dependencies on internal Defence resources.

Defence will process DISP applications in the following order; your business:

1. has a contract with Defence to support an ongoing Defence operation
2. has a contract with Defence
3. is planning to tender for a Defence opportunity, or in negotiations for a Defence opportunity
4. is applying for DISP with no existing relationship with Defence and no immediate tender opportunities.

Expected timeframes are as follows:

Membership level	Member context	Timeframes
Entry Level	Entity has all required clearances and certifications	2 – 3 months
Levels 1, 2 and 3	Entity has all required clearances, certifications and accreditations	3 – 4 months
All levels	Entity **does not** have all required clearances, certifications and accreditations	Depends on entity's level of security maturity

DISP processing is also dependent on internal Defence waiting times in the following areas (please note these timeframes are influenced by demand):

- Personnel security is dependent on AGSVA processing timeframes: https://www1.defence.gov.au/security/clearances/about/vetting-time-frames.
- Physical security may be dependent on the availability of DS&VS to conduct facilities inspections: https://www1.defence.gov.au/security/clearances.
- ICT and cyber security are dependent on the accreditation of networks by CIOG: https://www1.defence.gov.au/about/chief-information-officer-group.

INDUSTRY TIP

- If your ICT does not meet requirements for the appropriate level, you may want to consider whether employees with existing Defence clearances could use Defence PROTECTED Network (DPN) access (e.g. using a DREAMS remote access) while awaiting accreditation.
- Having a Defence or externally qualified trained Chief Security Officer and Security Officer can be helpful in facilitating the DISP timeframes.

7. What are the requirements for subcontractors/suppliers under DISP membership?

DISP members (especially large contractors) may use subcontractors to fulfil duties associated with Defence related work. Contractually, large contractors are responsible for ensuring that their subcontractors are aware of their DISP requirements.

Depending on the nature of the subcontracted work, this may require the DISP security requirements to extend to subcontractors. Industry entities working on Defence projects via a subcontracting arrangement with other industry entities are still subject to the same eligibility criteria when determining if DISP membership is mandatory.

If you are engaged or planning to engage in Defence classified work via a subcontracting arrangement, you are required to hold DISP membership to the appropriate levels required for that contract or project.

Additional information on supply chain security can be found at Annex C.

Chapter 3: Applying for Defence Industry Security Program membership

This chapter walks through the steps to apply for DISP membership. If you have not previously worked with Defence, obtaining Entry Level membership is a good first step. Most companies do not need higher than Entry Level membership unless they have a current or future contract with Defence specifying the need for a higher level. If there is any question about the level of membership required, advice should be sought from your Defence contract manager or from the DISP team at disp.info@defence.gov.au.

1. When is DISP membership required?

An appropriate level of DISP membership is required:

- when working on or with classified (PROTECTED or above) information or assets;
- when managing, storing or transporting Defence weapons or explosive ordnance;
- when providing security services for Defence bases and facilities; or
- if there is a Defence business requirement for DISP membership in the contract.

If you are a foreign entity you will not qualify for DISP, but your business may be recognised under a Security of Information Agreement or Arrangement (SIA). Website: https://ext.defence.gov.au/sites/default/files/media/security_of_information_agreement_or_arrangement_sia_fact_sheet.pdf.

NOTE

Even if DISP membership is not a requirement now, consider whether it may be beneficial in the future and to enhance the overall security posture of your business.

2. What are the steps to apply for DISP membership?

Before starting your application for DISP membership, ensure your business has the following:

A nominated Chief Security Officer (CSO) and Security Officer (SO) who meet the required criteria as set out in the table below.

A generic email address for all security related correspondence in the form of disp@insertbusinessname.com.au.

Ensure that your business ICT network meets **one** of the following accreditation standards:

- Top 4 of the ASD Essential 8 (specifically application control, patch applications, restrict administrative privileges and patch operating systems)
- ISO/IEC 27001 and 27002[5]
- NIST SP 800-171 (US ITAR requirement)
- Def Stan 05-138.

[5] ISO/IEC 27001 and 27002 are appropriate for the purposes of meeting DISP membership requirements. For specific applications, it is recommended that businesses also review additional standards under the ISO/IEC 27000 family of standards.

Use the following steps to apply for DISP membership

1. Familiarise yourself with 'Principle 16 and Control 16.1 - Defence Industry Security Program' of the DSPF: https://www1.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL.pdf.

2. Decide which membership levels are most appropriate for the type of work your business provides. At this stage, consider engaging with the Defence contract manager or the DISP team if required. You will also need to build your evidence that demonstrates that you meet the specified requirements for:
   a. Governance
   b. Personnel security
   c. Physical security
   d. ICT and cyber security.

3. Fill out the DISP application form and save to your computer: https://ext.defence.gov.au/security/industry-resources.

4. Fill out the DISP foreign ownership, control and influence declaration form and save to your computer: https://ext.defence.gov.au/security/industry-resources.

5. Email your completed forms to disp.submit@defence.gov.au.

NOTE

Following submission of your application Defence may contact you regarding the certification and accreditation of facilities and ICT systems.
Defence will also contact you about the outcome of your membership application once completed.

3. What level of membership do I need and what are the requirements?

The broad requirements and suitability matrix for each level of the DISP are outlined here and will be expanded further in the relevant chapters. The table below is extracted from the DSPF which provides additional context. See: https://www1.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL-Principle-16-Control-16.pdf and https://www1.defence.gov.au/security/industry/eligibility.

Membership level	Governance*	Personnel security	Physical security	ICT and cyber security

Entry Level	• Maintain an appropriate system of risk oversight and management i.e. risk register including security considerations
	• Provide business details
	• Provide points of contact
	• Must have a nominated Chief Security Officer (CSO) (must be able to meet AGSVA eligibility requirements for Baseline clearance)
	• Must have a nominated Security Officer (SO) (must be able to meet AGSVA eligibility requirements for Baseline clearance)
	• SO may request access to the DISP Security Portal, to access security documents, templates, forms and tools which include: assurance reporting forms, security policy and plans templates, risk assessment forms etc
	• Security Officer Training Course is optional for nominated SO and CSO, however the SO is to complete the Introduction to DISP course
	• Annual Security Awareness Course must be completed by all personnel
	• SO must understand and effectively manage personnel/facilities and
		• SO has no ability to sponsor security clearances
		• Provide a description of employment screening practices
		• AS 4811-2006 Employment Screening is the minimum standard for all new recruitments
			• Provide a description of physical security and access controls at each facility and their location	• Must meet one of the following standards across all of the entity's ICT corporate networks used to correspond with Defence:
				  ○ The following Top 4 requirements of the ASD Essential 8:
				  ▪ application control;
				  ▪ patch applications;
				  ▪ restrict administrative privileges; and
				  ▪ patch operating systems
				  ○ OFFICIAL / OFFICIAL: Sensitive network in accordance with the ISM/DSPF
				  ○ ISO/IEC 27001 and 27002
				  ○ NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (US ITAR requirement)
				  ○ Cyber security for Defence suppliers (Def Stan 05-138)
				• Provide a description of information and cyber security practices and accreditations

Membership level	Governance*	Personnel security	Physical security	ICT and cyber security
	information and cyber security up to an OFFICIAL/OFFICIAL: Sensitive level • Maintain and implement Security Policies and Plans • Insider threat program • Business security risk assessment • Reporting and management of security incidents and foreign contacts • Report changes in Foreign Ownership, Control & Influence • Conduct travel briefings • Complete annual assurance activities • Annual Security Report			
Level 1	All governance requirements from the Entry Level, plus: • Complete annual assurance activities • SO required to maintain a NV1 clearance • SO understands and effectively manages personnel / facilities and information and cyber security up to and including PROTECTED level • Security Officer Training Course is required for the SO, but optional for the CSO	All personnel requirements from the Entry Level, plus: • SO has the ability to sponsor Baseline security clearances • Ensure Baseline cleared personnel adhere to ongoing security clearance requirements	All physical requirements from the Entry Level, plus: • Ensure facilities are certified and accredited in accordance with the DSPF to receive, handle, store and destroy PROTECTED information and material	All information & cyber requirements from the Entry Level, plus: • Ensure a PROTECTED network or standalone device is employed in accordance with the ISM/DSPF

Membership level	Governance*	Personnel security	Physical security	ICT and cyber security
	• SO may request access to the Security Officer Dashboard for the ability to sponsor security clearances • Maintain a list of Designated Security Assessed Positions (DSAP)			
Level 2	All governance requirements from Level 1, plus: • SO must understand and effectively manage personnel/facilities and information and cyber security up to and including SECRET level	All personnel requirements from the Entry Level, plus: • SO has the ability to sponsor security clearances up to NV1 • Ensure Baseline and NV1 cleared personnel adhere to ongoing security clearance requirements • Ensure compartment holders adhere to compartment requirements	All physical requirements from the Entry Level, plus: • Ensure facilities certified and accredited in accordance with the DSPF to receive, handle, store and destroy SECRET information and material	All information & cyber requirements from the Entry Level, plus: • Ensure a SECRET network or standalone device is employed in accordance with the ISM/DSPF
Level 3	All governance requirements from Level 2, plus: • If applicable, SO trained in compartment briefings obligations – COMSO course • SO must understand and effectively manage personnel/facilities, and information and cyber security up to and including TOP SECRET level	All personnel requirements from the Entry Level, plus: • SO has the ability to sponsor security clearances up to NV2 • Ensure Baseline, NV1 and NV2/PV cleared personnel adhere to ongoing security clearance requirements • Ensure compartment holders adhere to compartment requirements	All physical requirements from the Entry Level, plus: • Ensure facilities certified and accredited in accordance with the DSPF to receive, handle, store and destroy TOP SECRET information and material	All information & cyber requirements from the Entry Level, plus: • Ensure a TOP SECRET network or standalone device is employed in accordance with the ISM/DSPF

Notes to table above:

- * Governance security must always match or exceed the highest level of membership sought for any other category.
- Source: DISP Suitability Matrix, Annex B of Control 16.1 DISP of the DSPF.

NOTE

An entity (such as a sole trader, partnership, trust, company or university) in the context of the DISP means an organisation that is registered as an Australian business and is located within the territory of Australia.

The DISP website also includes a decision matrix tool to assist in understanding the DISP membership level required, which can be accessed here: https://www.defence.gov.au/dsvs/industry/documents/DISP-Decision-Matrix.pdf.

4. How do I build my evidence to support my application?

Once you have determined the level of membership required, an assessment must be made against each security category to determine how closely the business meets the requirements, or if security improvements are required in some areas.

Under chapters 4 to 7 of this Guide you will find the specific requirements for each of the security categories. All documents and certification for each of the categories must be submitted with your application.

In summary, the table below sets out the questions you should address to assess your capacity to develop your application and build the required evidence.

Governance	
Does your organisation have a nominated Chief Security Officer (CSO) who is accountable for the security of your entity?	Yes or No
Does your entity have a nominated Security Officer (SO) (can be the same person as the CSO)?	Yes or No
If yes, do they have a security clearance and at what level?	Specify personnel security clearance level
Does your entity have Security Policies and Plans in place at the appropriate level of DISP membership which will be maintained and made available to Defence upon request?	Yes or No
Does your entity run an annual Security Awareness Program for all staff at the appropriate level of DISP membership and is this available to Defence on request?	Yes or No

Does your entity have an Insider Threat Awareness program suitable for the level of DISP membership and is this available on request to Defence?	Yes or No
Do the CSO and SO commit to their DISP reporting obligations? This includes maintaining a register of security incident reports, contact reports and overseas travel briefings, and will make this register available to Defence upon request.	Yes or No
Does your entity have a mechanism for the governing body, through the CSO, to approve the Annual Security Report and submit this annually?	Yes or No
If you are applying for DISP membership Level 1 or above for personnel security, can you confirm your entity maintains a list of Designated Security Assessed Positions, and will make this available to Defence upon request?	Yes or No
Personnel Security	
From the time of application for DISP membership, will all future business employment practices meet or exceed the requirements of employment screening standard AS 4811-2006, and be made available to Defence upon request?	Yes or No
Does the SO agree to support the entity's security clearance holders to uphold their clearance and compartments responsibilities? This includes, but not limited to: submitting change of circumstances forms, incident reports, contact reports and conducting overseas travel briefings.	Yes or No
Will your people be working in a Defence establishment? If yes, they may need a clearance as specified by the establishment.	Yes or No
Do your employees need a security clearance?	Yes or No
Do any of your personnel have a personnel security clearance?	Yes or No
If yes, what level of personnel security clearance?	Specify level of personnel security clearance
Physical Security	
Does your business need to use classified information and/or assets?	Yes or No
What is the highest level of classification your business needs to use?	OFFICIAL OFFICIAL: Sensitive PROTECTED SECRET TOP SECRET

Does your business have clear access control policy and permissions in practice?	Yes or No
Does this extend to any third party providers of goods and services?	Yes or No
Information and Cyber Security	
Will your information networks need to handle classified information?	Yes or No
What is the highest level of classified information your business needs to store, process or communicate?	OFFICIAL OFFICIAL: Sensitive PROTECTED SECRET TOP SECRET
Which standard does your entity's corporate networks meet?	• Top 4 of the ASD Essential 8 (specifically application control, patch applications, restrict administrative privileges, and patch operating systems) • ISO/IEC 27001 and 27002 • NIST SP 800-171 (US ITAR requirement) • Def Stan 05-138

5. Where and how do I submit my application?

Fill out the DISP application form (AE250) and the Foreign Ownership, Control and Influence (FOCI) Declaration (AE250-1) and submit to disp.submit@defence.gov.au. These forms can be found here: https://ext.defence.gov.au/security/industry-resources.

The application form must be completed by an individual with the authority to make assurances regarding your organisation's security practices. Defence recommends the DISP application form be completed by your Security Officer (SO) and approved by the Chief Security Officer (CSO).

6. What are my ongoing DISP membership obligations?

Once DISP membership has been granted, the CSO and/or SO may gain access to benefits such as the DISP Portal and the AGSVA Security Officer Dashboard which contain information on emerging security threats as well as further guidance to improve and maintain the security of your business. As a DISP member, you will be kept up to date with developments in the security space and will also be able to engage with other members to share lessons learnt.

As well as the benefits, DISP membership comes with ongoing responsibilities at every level, including:

- The requirement to submit an Annual Security Report (ASR);
- Undertake regular security training of staff including induction training for new staff;
- Respond and report any security incidents as soon as possible and maintain an accurate register of incidents and responses;
- Report any substantial changes as soon as possible, including changes in Foreign Ownership, Control and Influence (FOCI) status; and
- Ongoing employment screening and suitability checks.

The CSO must provide the ASR to Defence within ten business days of the anniversary of their original membership grant date. Failure to do so may impact on the business's DISP membership, including a review of their suitability, and potential downgrade, suspension or termination from the DISP. The template of the ASR can be accessed from the DISP website: https://ext.defence.gov.au/security/industry-resources.

As part of the ASR, Defence has created a checklist to ensure the DISP membership requirements are being met. The following checklist has been developed to assist you in completing your ASR. Please note not all of the requirements apply to all membership levels.

Governance	**Yes, No or N/A**
Entity has a nominated Chief Security Officer	Choose an item.
Entity has a Security Officer who has completed the Defence Security Officer training	Choose an item.
Entity has Security Policies and Plans	Choose an item.
Entity has reported security incidents and contact reports in accordance with the Defence Security Principles Framework (DSPF)	Choose an item.
Entity has reported any potential or actual changes in their Foreign Ownership, Control and Influence (FOCI) status	Choose an item.
Entity has provided annual security awareness training for staff	Choose an item.
Entity has an insider threat program available for staff	Choose an item.
Entity is maintaining an appropriate security register	Choose an item.
Entity has conducted overseas travel briefings in accordance with the DSPF and recorded details in their security register	Choose an item.
Entity is maintaining a list of Designated Security Assessed Positions (DSAP)	Choose an item.
Personnel Security	
Entity is screening new recruits against the AS 4811-2006 employment standard	Choose an item.
Entity is reporting change of circumstances and vulnerabilities for clearance holders to AGSVA	Choose an item.
Physical Security	
Entity is maintaining accredited facilities to receive, handle, store and destroy PROTECTED information and material	Choose an item.

Entity is maintaining accredited facilities to receive, handle, store and destroy SECRET information and material	Choose an item.
Entity is maintaining accredited facilities to receive, handle, store and destroy TOP SECRET information and material	Choose an item.
Information and Cyber Security	
Entity is continuing to meet the minimum information/cyber security requirements for Entry Level	Choose an item.
Entity is continuing to ensure any PROTECTED networks or standalone devices are employed in accordance with ISM/DSPF	Choose an item.
Entity is continuing to ensure any SECRET networks or standalone devices are employed in accordance with ISM/DSPF	Choose an item.
Entity is continuing to ensure any TOP SECRET networks or standalone devices are employed in accordance with ISM/DSPF	Choose an item.

7. Further questions

For information on DISP membership, contact Defence on:

Phone: 1800 333 362

Email: disp.info@defence.gov.au


A15-307
ARMY

Chapter 4: DISP governance requirements

1. About DISP governance

This chapter provides more detail about DISP governance requirements for your DISP application and participation in the program.

Good governance around security is achieved through having clear accountability and responsibility, suitable plans, processes and people in place to make sure your business is secure.

Good governance will help ensure you have appropriate practices across physical security, personnel security, cyber security, security education and training, and security incidents.

NOTE

It is important to note that your governance level for DISP membership needs to be the same as the highest level of your other requirements. That is, if you have Level 2 physical security requirements then you will need Level 2 governance requirements (on the assumption that is your highest requirement).

There are good reasons behind this emphasis on good governance. Governance documentation lays the foundation for security measures adopted by industry. It is important that your security risk assessment, security policies, plans and training reflect your business's ability to safeguard people, information and assets at the commensurate level.

Further, partnering with Defence may expose industry to additional threats. Working with Defence requires a strong security culture that mitigates risk and fosters a culture where security is in the forefront of everyone's mind. To best promote a security culture, DISP members are required to prepare governance documentation that identify:

- an appropriate system of risk oversight and management;
- clear lines of accountability;
- sound planning, investigation and response;
- assurance reporting and review processes; and
- clear escalation pathways.

2. Entry level governance requirements

To meet Entry Level governance requirements, you will need to:

1. Nominate a Chief Security Officer (CSO).
2. Nominate a Security Officer (SO).
3. Complete a business security risk assessment.
4. Ensure that you have current security policies and plans.
5. Implement a security risk register (or other system of risk oversight and management).
6. Report on Foreign Ownership, Control and Influence status.
7. Administer an annual security awareness program to your staff.

We take you through each of these steps below. You will also need to confirm that each of these steps has been completed in the DISP membership application form.

2.1 Nominate a Chief Security Officer (CSO)

The Chief Security Officer (CSO) has oversight and responsibility for security governance and championing good security culture within the business.

The CSO must:

1. Be a member of the organisation's board of directors (or similar governing body), executive personnel, general partner, or senior management official with the ability to implement policy and direct resources including maintaining a security register with board oversight.
2. Be an Australian citizen.
3. Obtain and maintain a minimum Baseline Security Clearance.

2.2 Nominate a Security Officer (SO)

The Security Officer (SO) works under the guidance of the CSO and is responsible for security activities including developing and implementing security policies and plans.

The SO must:

1. Be an Australian citizen.
2. Obtain and maintain a minimum Baseline Security Clearance.

The role of the CSO and SO may be conducted by the same person depending on the size and needs of the business.

IMPORTANT NOTE

Both the CSO and SO must be an Australian citizen and be able to obtain and maintain a Personnel Security Clearance at the Baseline level or above, as appropriate with the entity's level of DISP membership. Defence will sponsor the security clearance, in the first instance, for the CSO and SO, if required. The invoice for the cost associated with the security clearance will be forwarded by the AGSVA to your organisation for payment.

2.3 Complete a security risk assessment of your business

You will need to complete a security risk assessment of your business to:

- identify security threats or vulnerabilities to your business, including the impacted key assets;
- assess the impact of the threats and vulnerabilities; and
- decide how you will manage the risks identified i.e. whether to avoid, remove, accept or mitigate a risk.

You can access a template on how to complete a Security Risk Assessment (SRA) at Annex D. This is an example only and should be tailored to suit your business and individual circumstances. A more specific SRA should be maintained relating to any Defence contract the business is working on.

Further information on Defence's policy on SRAs can be found in the DSPF Governance and Executive Guidance document, paragraphs 31 and 40-41. In addition, a Security Risk Management fact sheet is located on the DISP website, and further information on SRAs is available on the DISP Portal.

DS&VS also provide a Security Risk Management Workshop to assist business with completing SRAs. To find out more information, contact ld.trainingnominations@defence.gov.au.

2.4 Develop security policies and plans

Following the security risk assessment, you will need to develop Security Policies and Plans for your business to:

- mitigate risks identified in your security risk assessment;
- address how your business will manage physical security, personnel security, ICT and cyber security, security education and training, and security incidents; and
- guide personnel in their security responsibilities.

The content of your Security Policies and Plans will depend on your business needs.

You can access a template on how to develop Security Policies and Plans – Entry Level here: https://ext.defence.gov.au/security/industry-resources.

NOTE

Security and engaging with risk: Your business needs to be prepared to engage in risk in order to proceed with day-to-day business. To meet your DISP obligations, you are required to implement an appropriate system of risk management and oversight. For example, your personnel need to know when they are empowered to accept risk or when they need to escalate it. The identification of your security risk tolerance and risk escalation pathways will assist you in meeting this requirement.

2.5 Implement a security register

A security register or other similar register of risk oversight and management must be implemented by DISP members.

A security register is a living document maintained by the SO to provide security oversight across governance, physical security, personnel security, ICT and cyber security, security education and training, and security incidents in your business.

A security register template can be found here: https://ext.defence.gov.au/security/industry-resources.

2.6 Implement an appropriate security system of risk oversight and management

Decisions on the nature and extent of security controls should be governed by the requirements of the DISP and the Security Risk Management system of your business.

The business should record and manage security information including, but not limited to, risk to the business such as:

- assets at risk;
- sources of threat;

- determine vulnerabilities;
- likelihood of the threat occurring;
- consequences of the threat if realised;
- apply controls; and
- assess residual risk.

ISO 31000 Risk Management provides the guide to such a system and is supported by Standards Australia HB 167 Security Risk Management.

2.7 Maintain an insider threat program

An insider threat program must be maintained by DISP members. It is important for the organisation and its personnel to understand the risk and factors of insider threats and receive practical guidance and ways to mitigate against such threats.

To assist organisations, an insider threat personnel security handbook developed by the Australian Government can be found here: https://ext.defence.gov.au/security/industry-resources.

Your insider threat program should have regard to ways to manage risk of insider threats and implement a proper framework to handle personnel security. Below is a framework that is an expansion of the Australian Government's insider threat handbook:

Organisational personnel security	Make sure you: • know your business • have a good security culture • perform a personnel security risk assessment • understand the legal framework • communicate personnel security and the consequences of personnel security breaches to your employees.
Pre-employment personnel security	Perform the following pre-employment background checks: • identity checks, including overseas applicants or applicants who have spent time overseas • dual nationality • contacts • qualification and employment checks including disclosure of any defence disclosure matters • national criminal history (police) checks • financial background checks • social media assessment. All documents for the checks should be secured. Any applicant who fails to meet the standard of your business should be rejected for employment.
Ongoing personnel security	Make sure you: • have access controls in place • perform protective monitoring • promote a security culture, including one that: ○ counters manipulation

	○ reports and investigates, when necessary ○ performs ongoing checks ○ submits contractors to the same security clearance as in-house personnel • recognise post-employment threats. Policies and Procedures: • ensure that the organisation's policies and procedures reflect the legal obligations. Employment contracts: • ensure that the organisation's employment contracts contain confidentiality obligations and provisions for continuous email supervision /access, social media monitoring, use of personal device (mobiles, tablets etc) obligations, travel obligations relative to security clearance, use or access to secured material at home, post-employment restraints.
ICT security	Be sure to consider and, if necessary, monitor: • electronic access • relevant policies and process around shared administrative accounts • account management policies and procedures • the standard operating environment • BYO device policies (including mobile phone, tablets, laptops, smart watches etc) • policies for at home devices and security issues (anything with a camera and microphone e.g. smart home devices etc) • system logs • Intellectual Property register.

Further consideration of personnel security is discussed in Chapter 5.

CASE STUDY

Malicious insider threat

A small to medium-sized company was reviewing its future plans as a Defence contract was coming to an end and there was concern about losing staff. A number of staff were actively looking for alternative employment, but one employee in particular had been openly critical on a range of company activities and felt they were "owed" by the company for their contributions.

In the employee's earlier stages of employment, they had been diligent and productive, but their performance had deteriorated as their colleague's contributions to the project were being recognised

over theirs (at least in their own eyes). Nevertheless, in the last month, the employee's work output seemed to improve despite some frequent absences from work.

Coinciding with this, the company's data transfer monitoring system, supported by a third party IT service provider, identified large amounts of material moving from the employee's unclassified computer by either USB or email. An examination of this identified that it was project related material, both in the employee's work area and from a larger area to which they had access. This led to a more detailed investigation that discovered that the employee was transferring this material to their home and additional email investigation identified that they were seeking employment with a competitor.

In the Defence industry, today's competitor is often tomorrow's partner and the CEO of the company had a collegiate relationship with their opposite number, so it was decided to raise the issue directly. It was discovered that the employee was not only taking and passing on the material as their own work but had already taken up part-time employment with the other company. Needless to say, this was a breach of the employment policies of both companies and the employee was terminated from these companies. The other company allowed the company's security and IT managers to work with its IT manager to clear all proprietary information.

What can you do to mitigate this situation?

The company must have:

- clear ethical guidelines;
- policies that provide clear guidance on acceptable behaviour;
- contracts (including employment contracts and non-disclosure agreements) that provide clear parameters for acceptable behaviour;
- a behavioural reporting system or whistle-blower scheme; and
- clear incident escalation processes.

The company should consider an insider threat program with the following characteristics:

- a profile of circumstances and relevant behaviours that would trigger initiation of a preliminary review;
- supervisors are briefed on indicators of potential triggers and characteristics of malicious insiders;
- Security and Human Resources work together to identify and assist those with potential triggers to help manage the issues driving them;
- investigative policy, framework and processes that will trigger an investigation and manage it effectively;
- investigative resources available in-house or by contract; and
- IT systems have monitoring, investigative and forensic capability.

2.8 Report on Foreign Ownership, Control and Influence status

As part of your application, you will fill out an AE250-1 form relating to Foreign Ownership, Control and Influence (FOCI).

The FOCI declaration is aligned with the Foreign Investment and Review Board (FIRB) and provides information to Defence contracting areas to support their security risk management activities.

Reporting on the FOCI status of your business involves disclosing any:

- Foreign directors
- Foreign board members
- Foreign shareholders
- Foreign revenue streams
- Agreements with foreign person(s)
- Foreign investments
- Subsidiaries with foreign directors or shareholders.

FOCI assessments support Defence contract managers to make informed decisions when assessing security risks associated with the procurement of goods and services from industry.[6]

To report on the FOCI status of your business:

1. Complete the FOCI (AE250-1) form: https://ext.defence.gov.au/security/industry-resources.
2. Submit the form to disp.submit@defence.gov.au with your application for DISP membership.

2.9 Administer an annual security awareness program to your staff

As part of your mandatory DISP requirements, you must administer an annual security awareness program to your staff. Material will be available on the DISP website which you may use to develop a package that is appropriate and proportionate to your entity's needs: https://ext.defence.gov.au/security/industry-resources.

Defence also hosts a Security Awareness Training course that will be available for SOs and CSOs seeking membership above Entry Level.

3. Higher level governance arrangements

For all governance requirements above Entry Level for DISP membership, you will need to work with Defence to be accredited to the right level. DS&VS can guide you in this process: disp.info@defence.gov.au.

The following are requirements associated with the following higher levels of security:

- For Level 1:
  - Entity meets requirements for Entry Level.
  - Entity must have appropriate security policies and plans up to PROTECTED.
  - At least one SO has an NV1 (SECRET) clearance.
  - Entity is required to hold a list of all cleared personnel on a DSAP list.
- For Level 2:
  - Entity meets requirements for Level 1.
  - Entity must have appropriate security policies and plans up to SECRET.
- For Level 3:

[6] For further information, see: https://ext.defence.gov.au/sites/default/files/media/foci_fact_sheet_d2.pdf.

- Entity meets requirements for Level 2.
- Entity must have appropriate security policies and plans up to TOP SECRET.

4. Ongoing governance obligations of DISP membership

There are a range of ongoing governance obligations that are required once you obtain DISP membership as follows:

1. **Report any changes in governance arrangements:** including, but not limited to, changes of appointment for the CSO and SO, and changes of reporting arrangements to the CEO or Board/Executive Committee.
2. **Submit an Annual Security Report:** to confirm continued compliance with DISP eligibility and suitability requirements (certification and accreditation).

   As described above, the CSO is required to report on the ASR annually from the date that the business was granted DISP membership.
3. **Participate in audit and assurance activities** conducted by the Defence Industry Security Office (DISO). More information on DISO audits is in Chapter 8.

Overseas travel

Security cleared personnel of the business that are contemplating business or private overseas travel are required to take the following actions:

- notify the SO about their travel plans;
- inform themselves about their destination via the Department of Foreign Affairs and Trade (DFAT) travel advisory (Smart Traveller website: https://www.smartraveller.gov.au/);
- if appropriate, be informed about classified intelligence on countries via DS&VS through the SO; and
- report any suspicious activity witnessed during travel to their SO to enable reporting to Defence (including reporting security contact concerns via the XP168 form).

For overseas travel of personnel, their SO is responsible for:

- briefing personnel prior to travel;
- recording the travel in the Security Register; and
- debriefing the personnel upon return from travel.

The SO is also responsible for providing personnel with a clean mobile phone / laptop that contains no secured data or materials.

Travel briefing should also include (but not limited to):

- relevant export controls (see Ai Group Defence Council Australian Guide to Export Controls and Best Practices for further information: https://www.aigroup.com.au/business-services/industrysectors/defence/exportforum/australian-export-best-practice-guide-2020);
- social media training;
- cultural issues where applicable;
- social interaction training; and
- protocols in relation to security of devices while traveling.

To assist in recording overseas travel of personnel in and out of Australia, the applicant can make a request of international movement records from the Department of Home Affairs by completing a 1359 form, which is available here: https://immi.homeaffairs.gov.au/entering-and-leaving-australia/request-movement-records. Supporting documents, including proof of identity, will be required to complete this form. The applicant can either be the travelling personnel, or another person requesting on their behalf or seeking information about them. If the applicant is another person, they will need to receive written authorisation from the personnel. This request will only cover travel records after 1981. (For movements records prior to 1981, the applicant will need to contact the National Australian Archives at https://www.naa.gov.au.) The completed form can be submitted to request.movement@homeaffairs.gov.au.

ITAR: if undertaking projects or activities where ITAR is applicable, please refer to the specific requirements for security, travel and transfer of secured materials under that regime.

INDUSTRY TIP

If the application is approved by the Department of Home Affairs, the type of information provided in the report is a list of travel dates and flight numbers. The applicant will need to look up the flights online to map the countries that were visited.

For further information, see:

- DSPF Control 44.1 Overseas Travel
- Security Toolkit on the DISP Industry Portal via DOSD

Official domestic travel

For domestic travel of personnel, the SO will need to consider whether their personnel need access to a particular facility, and that they have appropriate security clearance or briefing.

Official overseas travel

If personnel are officially travelling overseas, they are required to advise their SO.

If personnel are travelling to a country where Australia has an SIA that may involve access to classified information or access to a facility requiring a security clearance, they need to complete an XP090 form (found via the DISP Portal). This form will need to be submitted to their SO and sent to the AGSVA at securityclearances@defence.gov.au. Generally, request for visits take a minimum of 20 business days for processing. For specific lead times, please refer to the relevant SIA.

CASE STUDY

Travel cyber threat

An engineering consultant for a small to medium-sized business had been travelling through Asia on a long-term project. As is the nature of frequently travelling overseas and meeting deadlines, the consultant would spend part of their time working at airports while waiting for their next flight.

The business had security measures in place and had trained their team on what they needed to do to make sure confidential information was not compromised.

During the consultant's third consecutive trip, their mobile phone was on low battery and they needed to make an urgent phone call while in transit to close a contract that had a fixed deadline with an important client. Finding an unused public USB port near an airport cafe, they ordered a coffee while waiting for their phone to be charged.

When the consultant's phone was sufficiently charged, they attempted to make a call but found that their phone had been locked out and they were unable to get back in. With their plane now due to depart, the consultant was unable to make their urgent phone call and almost lost business with their client.

It took the business two weeks to identify that the consultant's phone had been compromised with malware which had locked them out after they connected it to the airport's public USB port. Luckily, no information was stolen from the mobile on this occasion.

Even though the business had security measures in place and their people were trained, they realised that they did not take into account this scenario and could not rely on people to always remember to do the right thing.

What can you do to mitigate this situation?

- Review procedural measures and associated staff awareness content to ensure staff understand the risk, their responsibilities and to be more alert while travelling.
- Ensure all your IT products run the latest protection software that monitors and reports suspicious activity in real time and keep this software updated.
- Consider the different environments your people work from and include these in your risk assessments and put in place measures to mitigate these risks.
- Assess the risks introduced by the different devices your employees use for work, not only the work laptop.
- Consider using alternative devices (in this case with superior battery life) or providing a portable power bank for staff that travel regularly to avoid using public USB ports, and include this control (if implemented) in your risk assessment.

Chapter 5: DISP personnel security requirements

1. About DISP personnel security

This chapter provides additional information on personnel security for your DISP application and participation in the program.

Personnel security is about ensuring your employees and contractors are suitable to access government information and assets, and meet an appropriate standard of security competence, integrity and honesty.

Effective personnel security will help protect against threats to your business from trusted insiders and help to protect your intellectual property. It involves collaboration between human resources and security within a business.

DISP personnel security requirements can assist your business to have:

- current and potential employees (and contractors) that can access national security information and assets; and
- suitable cleared personnel to work with Defence information and assets.

There are three core principles from the Australian Government's Protective Security Policy Framework (PSPF) that you must implement to meet DISP personnel security requirements. You must:

1. Ensure eligibility and suitability of your personnel requirements to have access to classified Government resources through Australian Government Security Vetting Agency (AGSVA) vetting protocols.
2. Manage the ongoing suitability of personnel requirements and report any information that may be of security concern.
3. Ensure that separating personnel have all their access to Government information revoked and inform AGSVA of this separation immediately.

2. Applying for DISP membership – personnel security and membership levels

Choosing the DISP level for personnel security depends on the level of security classified information or physical assets that is being sought. Your people will need the corresponding personnel security clearance level to access that information or physical asset.

The table below shows the requirements for each personnel security level.

Membership level	Personnel security requirements
Entry Level	The business's employee meets the Australian Standard for Employment Screening (AS 4811-2006): • An identity check requiring 100 points of ID; • Address history checks for a minimum of five years; • Character reference checks; • A national police check not exceeding one year; • An Australian Securities and Investments Commission (ASIC) check (where relevant); • Checks on all declared experience and qualifications; and • Social media assessment. Entity will maintain records of all employees.
Level 1	Meets requirements from Entry Level. The business can sponsor clearances up to Baseline (check DSAP list for employee clearance levels). At least one SO has an NV1 clearance.
Level 2	Meets requirements from Entry Level. The business can sponsor clearances up to NV1 (check DSAP list for employee clearance levels). At least one SO has an NV1 clearance.
Level 3	Meets requirements from Entry Level. The business can sponsor clearances up to NV2 (check DSAP list for employee clearance levels). At least one SO has an NV1 clearance.

3. Personnel security requirements for entry level

You will need the following for Entry Level personnel security requirements:

- Ensure your CSO and SO hold a minimum Baseline clearance level;
- Implement the AS 4811-2006 Employment Screening standard into your employment screening practices;
- Provide a description of employment screening practices;
- Ensure employment agreements contain all necessary terms and conditions reflecting security obligations; and
- Maintain a record of employees.

For levels above Entry Level, you will need the additional requirements as listed in the table above, corresponding to Level 1, 2 or 3 (as appropriate).

3.1 Ensure your CSO and SO hold a minimum baseline clearance level

You will need to ensure both your Chief Security Officer (CSO) and Security Officer (SO) hold a minimum Baseline clearance level. Refer to Chapter 4 for details on who can be a CSO and SO in your business.

In order to obtain a Baseline clearance, your CSO and SO will need to be sponsored by a government agency (generally Defence for DISP membership).

If you do not have a current contract with Defence:

- Contact the DISP team on disp.info@defence.gov.au to discuss your sponsorship options.

If you are in contractual negotiations to work with Defence:

- Discuss sponsorship options with your Defence contract manager during the contractual process.

For information on getting an Australian Government security clearance view the AGSVA website: https://www1.defence.gov.au/security/clearances.

3.2 Implement the AS 4811-2006 – Employment Screening standard into your employment screening practices

Pre-employment screening, in line with AS 4811-2006 Employment Screening standard, is essential for your DISP membership at Entry Level and above.

You must read the Employment Screening standard and implement those in your workplace. In summary:

- An identity check requiring 100 points of ID;
- Address history checks for a minimum of five years;
- Character reference checks;
- A current national police check;
- An ASIC check (where relevant);
- Checks on all declared experience and qualifications; and
- Social media assessment.

Other activities to consider as appropriate, especially in the pre-employment process, include:[7]

- Eligibility to work in Australia;
- Employment history checks including Defence related work;
- Residential history checks;
- Referee checks;
- Personal employment contracts;
- Non-disclosure agreements; and
- Non-compete clauses.

Employment screening applies to security cleared and non-security cleared personnel, contractors and others who will have access to Australian Government resources.

[7] Note: This is a different process to the AGSVA vetting process.

INDUSTRY TIP

Past employment history

- Your HR processes must ask potential staff to advise of any prior Defence related history that may impact their employment. While the staff member may still not report such matters you must ensure you ask.
- Depending on the type of incident, it is wise for your SO to ask Defence if there have been any reportable incidents in the staff member's past and if so, what measures should the company put in place.
- Your Employee Handbook must provide clear instructions to employees related to their obligations while with the company and under the DISP. They must be required to read the Security Practices and Procedures manual on a routine basis.
- For example, your Employee Handbook must clearly advise employees of all ICT activity on your server which is your property and you will randomly access email records from time to time. Have an ICT use policy in your Employee Handbook. This would be complemented by taking appropriate measures to safeguard your IP and any Defence information you have.
- Ensure the Employee Handbook also contains policies in relation to BYO device, social media and email assessments that the company will undertake from time to time.

3.3 Provide a description of employment screening practices

You will need to provide details of how potential employees are screened.

This may be as simple as a list of actions that you are taking documented in your policies and procedures. The lists above in section 3.2 provide suggested actions.

Refer to the Privacy Act as this may be applicable in relation to disclosure of any personal information collected in the process of employment screening (see reference in Annex A).

4. DISP obligations – obtaining and maintaining personnel security clearances

As part of the DISP membership application process, you must certify that your SO agrees to support your entity's security clearance holders to uphold their clearance and compartment responsibilities. This includes, but is not limited to: submitting change of circumstances forms, incident reports and contact reports, and conducting overseas travel briefings.

Personnel security clearances are necessary for personnel that need access to classified material or access certain classified work areas while working with the Commonwealth. A clearance may also be necessary where an individual may work in a position of high responsibility, or may have delegations and duties that, if mishandled or abused, could cause Defence or your organisation considerable harm or reputational damage.

These clearances are a snapshot in time that must be revalidated at regular intervals (as shown below) or if circumstances change.

Information up to and including:	PROTECTED	SECRET	TOP SECRET	CAVEATED & CODEWORD
Baseline Vetting	Revalidated after 15 years			
Negative Vetting 1 (NV1)	Revalidated after 10 years			
Negative Vetting 2 (NV2)	Revalidated after 5-7 years			
Positive Vetting (PV)	Revalidated after 5-7 years. Appraisal every year.			

The Australian Government Security Vetting Agency (AGSVA) provides a Security Clearance Applicant Guide Book to assist clearance applicants which can be found here:

https://www1.defence.gov.au/Security/Clearances/Resources.

NOTE

As a result of the Espionage and Foreign Interference Act 2018 it has become a federal offence to provide false information during the security clearance process. Providing false information can lead to large pecuniary penalties and a possible prison sentence term of up to five years' imprisonment.

4.1 Sponsoring security clearances

The SO is responsible for sponsoring personnel security clearances. The exception is where the entity only holds Entry Level personnel security – in this scenario, the Government agency will sponsor.

Eligibility to Sponsor

Your SO or CSO has the ability to sponsor higher security clearances if they are accredited at the following levels for personnel security*.

* Be aware that sponsoring a security clearance begins the clearance process. It does not guarantee that a security clearance will be granted.

Entry Level	Level 1	Level 2	Level 3
No ability to sponsor security clearances.	Sponsor security clearances up to and including Baseline.	Sponsor security clearances up to and including NV1.	Sponsor security clearances up to and including NV2. Only a SES Band 3/3 Star can sponsor an individual to a PV clearance level.

4.2 Time and costs considerations of personnel security clearances

Cost of the employment screening standard AS 4811-2006: Secure PDF ($50.72); Printed Edition ($56.30); or Printed Edition + PDF ($71.01).

DISP members are financially responsible for all costs associated with their staff's security clearances.

AGSVA will issue invoices monthly for all finalised security clearances. Payment is due within 30 days from the date of invoice. Late payment might see a clearance suspended until full payment has been received.

Business Days*:	20	90	125	180
Baseline Vetting	$637.67 AUD*			
Negative Vetting 1 (NV1)	$1,327.27 AUD*			
Negative Vetting 2 (NV2)	$2,267.54 AUD*			
Positive Vetting (PV)	$10,713.95 AUD*			

* Personnel security clearance timeframes and costs are reviewed by AGSVA on a yearly basis. Timeframe and costs are true at time of publishing; however, check AGSVA's website for the most up-to-date figures.

Further information about AGSVA personnel security clearance timeframes can be found here: https://www1.defence.gov.au/security/clearances/about/vetting-time-frames.

5. Foreign nationals

Any foreign worker who needs access to Australian Government classified resources is required to hold a security clearance recognised by the Australian Government. This can occur in the following ways:

For all sponsoring entities:

A security clearance issued by AGSVA or another authorised vetting agency granted under a *citizenship eligibility waiver* approved by the sponsoring entity.

OR

For the Australian Department of Defence, or those supporting Defence contracts:

A foreign national security clearance acknowledged by the Australian Government under a *Security of Information Agreement or Arrangement (SIA).*

Visit the Defence Industry Security page (https://ext.defence.gov.au/security/industry-resources) if you would like more information about:

- countries with a SIA with the Australian Government;
- engaging overseas workers with classified Defence contracts; and
- membership of the DISP.

CASE STUDY

Exit processes for employees and contractors

A small to medium-sized enterprise contactor underwent a significant transformation in terms of personnel.

The contractor's former head of security retired and received a handsome redundancy package. The former employee had been with the company for over a decade and left on good terms. In the employee's last week, they forgot to hand over their security pass to their security team, but the company did not follow up with revoking the former employee's access.

A few months later, the business's security guards identified a security breach. When they investigated, they identified that the former employee's pass had been used to access the site in the evening after their departure. The business reported it to the police, who arrested the former employee on suspicion of trespassing and theft.

A few days later, the former employee was released and their ex-partner was arrested. It turned out that the ex-partner had used the former employee's pass to gain access to the premises without their knowledge and was captured on a neighbouring business' CCTV.

What can you do to mitigate this situation?

- Consider ways in which your employees may be targeted as trusted insiders and include these examples in your mandatory and ongoing awareness training for all staff.
- Regularly review whether the level of security on premises is appropriate for protecting your information or assets and employees, and update your risk assessment if any changes are made.
- Instead of relying on neighbouring businesses, install video surveillance for entries and key areas at the site.
- Ensure your separation process for staff leaving the organisation includes the removal of your employee's access (both physical and ICT).
- Ensure that your exit processes catch, review and remove access for part time staff, contractors and service providers who no longer need access.

Ongoing personnel security obligations of DISP membership

There are a range of ongoing personnel security obligations for DISP membership:

1. Report any changes to personnel security to the DISP team.
2. Conduct pre-employment screening in line with AS 4811-2006 Employment Screening standard.
3. Report on travel using the AB644 form before and on return.
4. DISP members must report all foreign contact (suspicious, ongoing, unusual and/or persistent contact with a foreign national(s)), in accordance with Defence Policy (see DSPF Principle 45 – Contact Reporting).
5. Maintain a Designated Security Assessed Position (DSAP) list, which identifies specific positions that require a certain level of clearance.
6. Your business will also need to assess and manage the ongoing suitability of personnel requirements at all levels and report any information that may be of a security concern. You can access templates on how to complete a Personnel Security Assessment at Annexes E.1 and E.2.

   This includes reporting on changes in the personal circumstances of the personnel. Depending on their security clearance level, the person's clearance will need to be revalidated accordingly. The SO can assist employees to complete their applications and flag when clearances are due for revalidation, however, it is the clearance holder who is responsible for their own security clearance and required reporting.

   Both employers and security cleared personnel have responsibility for managing the ongoing suitability of security cleared personnel.

Employer responsibilities

Entities are required to report a change in personal circumstances of the personnel that may impact on their continued suitability to hold a clearance. This should be reported to the AGSVA via the SVA004 form: https://www1.defence.gov.au/Security/Clearances/Resources. For example, the circumstances relating to concerning behaviour such as changes in personality, alcohol or drug misuse, and criminal or illegal activity.

Security cleared personnel responsibilities

Security cleared personnel are required to meet their responsibilities on an ongoing basis in order to continue being suitable to hold security clearance. If there is a change in personal circumstances, the security clearance holder should report this to their SO, who in turn is required to report this to their sponsoring business and AGSVA via the SVA003 form: https://www1.defence.gov.au/Security/Clearances/Resources.

Examples of changes in personal circumstances include overseas travel, relationship status, living arrangements and finances.

Clearance holders must advise their SO of any planned overseas travel to arrange the necessary travel briefings and record the travel in the Security Register.

While this is a specific ongoing obligation for the CSO and SO, it is prudent for all managers and supervisors to monitor their employees for any concerning behaviour.

A company may give consideration to a manager's security obligations as part of their duty statement. The company may also consider these risks and reporting requirements as part of their staff workplace performance assessments.

Examples of concerning behaviour include:

- Changes in personality or workplace behaviour/relationships
- Misuse of alcohol or other drugs
- Criminal or illegal activity
- Indicators of financial instability or sudden, unexplained wealth
- An active gambling habit
- Disclosures on social media.

If managers or supervisors observe concerning behaviour, they must inform the CSO or SO. This will enable the CSO or SO to commence preliminary enquiries and report on the security concerns and incidents to Defence (see DSPF Principle 77 – Security Incidents & Investigations). This may lead to the entity undertaking specific security measures to address the concerns or incidents.

Clearance holders have an obligation to report other clearance holders when there may be implications for security.

Obligations will be discussed in more detail in the Security Officer Training course.

CASE STUDY

Insider threat

(from Insider Threat Handbook)

Melissa had worked for a small pharmaceutical laboratory for 12 years, almost since its inception. She was well known and well liked, mostly because she was good fun. Everyone knew she liked the local clubs for a drink and dabble on the pokies.

In January, Melissa came back to work from Christmas holidays less motivated than normal. Word got out that she had separated from her husband. During the next few months, Melissa's demeanour and behaviour changed; she often arrived late and left early, and she was distracted and took a lot of calls outside on her mobile phone. Everyone put this down to the separation.

One weekend, the laboratory was burgled, and a large volume of a chemical used to produce methamphetamines was stolen. There appeared to be no sign of forced entry. Melissa called in sick that week, but no one took too much notice.

The following week, Melissa was arrested. The company's CEO called a staff meeting to explain that Melissa had amassed a serious gambling debt and, in the process, dealt with a well-known criminal network. She was not able to repay some of her debt and, with her and her family's safety under threat, had provided access to the thieves.

The CEO told staff that Melissa was very apologetic and upset when interviewed by police. She also said she had tried to send signs to a few colleagues that she was in trouble as she was too scared to tell anyone directly. She pleaded guilty and was sentenced to six months in prison. Her husband took custody of their three children, and their house was sold to repay some of the debt. The chemicals were never recovered.

What can you do to mitigate this situation?

- Identify significant changes in an employee's personal circumstances.
- Note when an employee seems under considerable stress.
- Check whether all employees need after-hours access.
- Support and engage with the employee throughout periods of stress.

6. Conduct security training of personnel

See the section on security governance for information about training of personnel on security awareness, insider threat awareness, and SO training.

In addition, ensure your employees are aware of the risks associated with international travel while conducting official business or on holiday.

Pre and post trip briefings are required.

Check what personal devices employees are bringing to work and ensure that they understand risks associated with these devices.

As part of your insider threat awareness program you may want to include training for staff.

The Australian Government's insider threat handbook can be used to develop this training.

Chapter 6: DISP physical security requirements

1. About DISP physical security

A safe and secure physical environment helps to prevent or mitigate threats or attacks against Defence facilities, personnel, and security protected information and assets. Physical security measures and procedures have been evolving as new threats have emerged, driven by advancing technology and requiring human ingenuity to appropriately respond. While there is a lot of attention being paid to modern cyber security threats, physical security is still a critical part of the defences of your business.

There are three underlying principles in developing physical security for your business:

DETER – Deterrence measures are those that cause significant difficulty or require specialist knowledge or tools for adversaries to defeat. Deterrence measures include fencing and advertising your security measures.

DETECT – Measures that identify unauthorised action that is being taken or has already. Detection measures include alarms, CCTV and you identifying/questioning people in a restricted zone.

DELAY – Measures to impede an adversary during attempted entry or attack. Delay measures include implementing multilayer measures, for example fencing, access passes, safes and the need to know.

2. DISP levels for physical security

The type of DISP membership for physical security will depend on the level of security classification for the information or physical asset that is being held at the physical location. These are summarised in the table below.

	OFFICIAL / OFFICIAL: Sensitive	PROTECTED	SECRET	TOP SECRET
Entry Level	Must be able to provide a description of physical security and access controls at each facility.			
Level 1	Ensure facilities are certified and accredited in accordance with the DSPF to receive, handle, store and destroy PROTECTED information and material.			
Level 2	Ensure facilities certified and accredited in accordance with the DSPF to receive, handle, store and destroy SECRET information and material.			
Level 3*	Ensure facilities certified and accredited in accordance with the DSPF to receive, handle, store and destroy TOP SECRET information and material.			
	* For Level 3 membership you will not need to have a Secure Compartment Information Facility (SCIF) unless stipulated in a contract and you are sponsored by an SES Band 3 or equivalent.			

3. Steps to DISP membership – physical security and compliance

In order to understand and meet your physical security requirements for DISP membership you will need to consider the following:

1. Identify the information or physical assets that are being protected and the required security classification and/or business impact level.
2. Conduct a security risk assessment of the sites/facilities that are being planned to store and/or use the information or physical assets. This will require a holistic security assessment including physical security and personnel security. You can access a template on how to complete a Physical Security Assessment at Annex F.

3. Determine the appropriate physical security zone(s). This will include consideration of relevant physical security measures. Take a 24/7 approach to all security obligations – not just in relation to working hours.
4. Determine appropriate DISP level membership for physical security (note: personnel security will also be required). A key consideration is the level of sensitivity of the information or asset and how that is handled by the business e.g. storage, how the asset will be used etc.
5. Certify and accredit the appropriate physical security zone(s). Self-certification for Zone 2 is permitted with DS&VS accreditation. For Zones 3 to 5, the DISP Team's involvement will be needed with respect to certification and accreditation.
6. For your DISP membership form, you will need to list the physical addresses of all your business facilities, including any located outside of Australia.

INDUSTRY TIP

Cost-benefit analysis

In determining your physical security DISP membership level, it will often be important to conduct a cost/benefit exercise. For example, an SME contractor currently delivering classified work to Defence might submit an upgrade request for physical security membership under their existing DISP membership, in hopes that they could deliver elite TOP SECRET services to Defence.

As per the suitability matrix,[8] the company must ensure their chosen facility is certified and accredited in accordance with the DSPF to receive, handle, store (and for what length of time) and destroy TOP SECRET information and material to meet Level 3 physical security DISP membership.

The Defence Security and Services (DSS) team would inspect the facility and advise on necessary upgrades to meet certification and accreditation requirements for a Zone 5 facility able to store TOP SECRET information.

In this scenario the costs to upgrade may be prohibitive.

In this scenario you might:

- Consult with your contract manager to determine the level of classification for your Defence contracts and secure your company's facility accordingly.
- Conduct a cost/benefit analysis to determine if your business wants to invest in upgrading their facilities to accommodate an upgrade of DISP membership.
- Contact yourcustomer.service@defence.gov.au for queries relating to potential physical security upgrade for your business.

[8] Suitability Matrix: https://www1.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL-Principle-16-Control-16.pdf.

3.1 Identification of the information or physical assets that are being protected

Entry Level DISP members are required to notify DS&VS of the physical security arrangements at each facility as part of the membership application process. The DISP website provides a Security Policy and Plans (SPP) template which includes examples of the type of physical security and access control considerations that Entry Level DISP members should describe for each of their facilities. These can be accessed here: https://ext.defence.gov.au/security/industry-resources.

For a more detailed physical security assessment template see Annex F. This template provides an indication of the kinds of issues you might consider when assessing your physical security measures and DISP membership requirements. The template is an example only and will need to be tailored to your specific needs.

NOTE

The DSPF Principles 72-74 provide important context and guidance on physical security: https://www1.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL.pdf.

3.2 Physical security zones and the certification/accreditation process

As part of your DISP membership application you will be asked whether your facilities hold physical security certification and/or accreditation.

Physical security zones describe areas on a site that process, handle and store security-protected assets. The purpose of the physical security zone methodology is to establish scalable levels of physical security protection.

The physical security zones do not directly correlate with DISP level of membership for physical security. However, the classification of information and assets (including business impact level) located in a particular physical security zone will affect the way in which the DISP member can handle that information or asset.

3.3 What are the physical security zones and how are they certified or accredited?

The physical security zones are as follows:

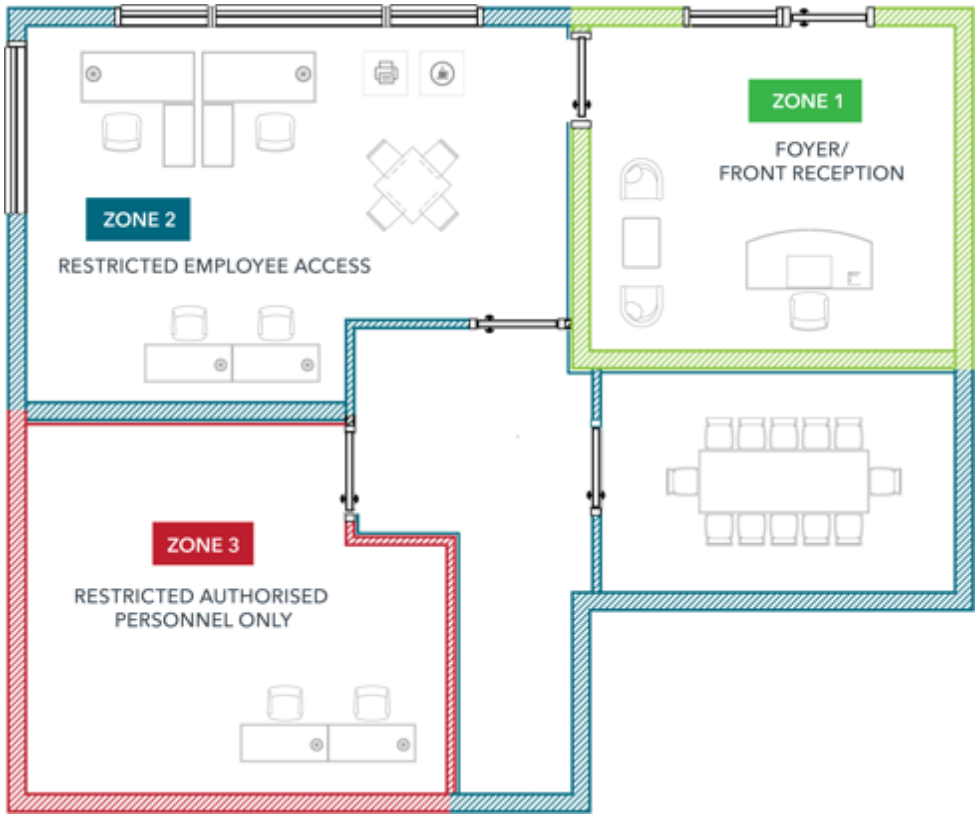
- **Zone 1** is a public access area within a space or area that has access control measures in place at the perimeter. No certification or accreditation is required for Zone 1.
- **Zone 2** facilities are considered low-risk and commonly recognised as normal office buildings constructed in accordance with the Building Code of Australia, with commercial locking and restricted profile keying systems along with other requirements outlined in the guidelines. The perimeter of Zone 2 facilities are generally slab-to-slab construction or tamper evident ceilings after hours. Zone 2 can store up to certain levels of classified information and assets in accordance with the PSPF. Businesses may be able to conduct a Zone 2 self-certification, with support from DS&VS who will complete the final accreditation.

- **Zone 3** facilities have limited employee and contractor access with visitors escorted within the zone. Ongoing employees in these facilities are to hold the security clearance at the highest level of the material they access within the zone. Storage of information up to SECRET (and equivalent Security Protected Assets (SPAs)) is permitted, provided they are stored within security containers specified within the DSPF/PSPF for the level of material held within the zone.
- **Zone 4** has strictly controlled employee access with personal verification as well as card access. Only contractors and visitors with a need-to- know that are closely escorted are provided access. Where security classified information is stored within the zone, all employees with ongoing access are to hold a security clearance at the highest level of the information held within the zone. SPAs with a business impact level of catastrophic can be stored within this zone.
- **Zone 5** has strictly controlled employee access, with personal identity verification as well as card access (dual authentication access). Visitors and contractors with a need to know are closely escorted at all times. Employees with ongoing access to the area are to hold a security clearance and briefings at the highest level of the information held within the zone. Zone 5 areas are where information classified at TOP SECRET, codeword information or large quantities of SECRET information is stored and used or where the aggregate of information would have a catastrophic business impact if compromised.

A more detailed comparison of the zones and DISP membership levels can be found at Annex G.

Example of physical security zones

The following diagram provides an example of the setup of a layered approach to physical security zones within an organisation's premises.



4. Physical security measures to protect your business

Once you have determined the required physical security zones, you will need to consider the relevant physical security measures for each zone category.

Each physical security zone will have its own requirements for the types of physical security measures put in place. The choice of measures will depend on the security risk assessment undertaken by the organisation in handling the particular information or assets that requires protection. Each assessment will likely be different, given the varying nature of each site/location.

Physical security measures include:

- Walls
- Barriers and signs that deter and delay unauthorised entry
- Security alarm systems that detect attempted or unauthorised access and alert someone to the need to respond
- Access controls that restrict based on security clearance and need to know
- Mechanical locking devices and access control systems operated by keys or codes
- Restricted areas
- Documented access procedures
- Security/staff physically located at entry and exit points, and staffed reception point
- Security/staff who monitor and control entry and exit points using intercoms, videophones, and CCTV
- CCTV
- Electronic access control systems (EACs)
- Authentication factor and dual authentication
- Identity cards
- Security keys
- Security zones, rooms and containers that protect SPA including classified information.

A useful summary of the minimum and/or recommended standards expected for each physical measure that should be implemented at each physical security zone is available from the PSPF: https://www.protectivesecurity.gov.au/sites/default/files/Table-3-physical-protections-for-security-zones.pdf; https://www.protectivesecurity.gov.au/sites/default/files/Table-3-physical-protections-for-security-zones.DOCX.

The CSO or their delegated security adviser are required to obtain from Defence certification and accreditation for the physical security zones. A useful summary of the CSO's (or their security adviser's) role relating to physical control measures within physical security zones is available in PDF and Word versions:
https://www.protectivesecurity.gov.au/sites/default/files/2019-09/policy_16_-_table_4_-_summary_of_control_measures_and_certification_authority.pdf;
https://www.protectivesecurity.gov.au/sites/default/files/2019-09/policy_16_-_table_4_-_summary_of_control_measures_and_certification_authority.docx.

The Security Construction Equipment Committee (SCEC) is also responsible for maintaining an approved list (Security Equipment Evaluated Products List (SEEPL)) of protective security products that can be used, mainly in Zones 3 to 5. Access to this list is available through application by DISP members and ABN registered companies working on Australian Government projects via:
https://www.scec.gov.au/catalogue.

Further information on additional physical security measures relating to security containers and cabinets, Security Alarm Systems (SAS), security guards and ICT facilities are provided in Annex H.

5. Ongoing physical security obligations of DISP membership

It is important that your business has an ongoing maintenance program for your physical security. Any changes to your physical security should be reported to the DISP team.

Examples of ongoing maintenance and obligations of physical security include:

- **Audit your facilities' keys every six months.** A key register must be maintained by the SO and an audit of your facilities' keys is required every six months. Duplicate keys are not to be made except on the authorisation of the SO and recorded in the key register. The loss or compromise of a security key must be reported in accordance with DSPF Principle 77 – Security Incidents and Investigations using the online form XP188 Security Incident Report.
- **Keep up to date records of your security containers.** Your SO is to record details of the security containers, their locations and their custodians in the Security Register.
- **Keep Security Alarm Systems maintained.** Your Security Officer is to ensure that the SAS is installed, operated, maintained and monitored in accordance with the manufacturer's specifications and, where applicable, Australian Government specifications. All alarm incidents and response actions are to be reported to the SO. The SO shall investigate all reported incidents, provide advice and take necessary action to correct any security deficiencies immediately. Details of alarm incidents and response actions will be recorded in the Security Register.
- **Keep guarding instructions and procedures up to date.** Your SO is to ensure that detailed guarding instructions are provided to your guarding organisation (as appropriate). Your SO should ensure that the instructions are kept up to date and that a backup procedure is in place. You should also ensure that the guards and other members of the response team are briefed on their role, and the response and reporting actions required of them in the event of an emergency or other reportable incident.

IMPORTANT NOTE

Accreditation of physical security zones may cease if:

- The accreditation expires (ten years for Zone 2 and five years for Zones 3-5).
- There is a change to the level of information or assets associated with the area or in the business impact level related to the security classified information or physical asset located in the zone.
- Significant changes are made to the facility or physical security controls.
- There are other circumstances outlined by the accreditation authority.

CASE STUDY

Tailgating and access control

The threat of unauthorised entry is an obvious one, yet it often fails to receive enough attention from staff. The impact can be anything from theft to cyber attack or even physical attack on employees.

A company was managing a high-level technical site with aerospace capability. Security measures in place at this site relied on access control for managing staff and visitor entry, including a receptionist controlling the inner access and pass requirements entry logs.

A criminal team with two entry specialists devised a process to access the site, which was based on observations over time of a vulnerability in the company's security procedures whereby personnel were heavily preoccupied towards the company's business closing hours. They would monitor the timing of exits at close of business and look for an opportunity to access as people left. The entry team consisted of a professionally dressed man and woman who would approach the area when the reception had closed and wait a few seconds for the inner door to open. They also identified a back exit to the carpark which they noticed allowed personnel to leave by this method at the end of the day.

Walking in through the front door, as if they were regular attendees, they would walk through the work area following a set route and identify any unsecured laptops or full laptop bags, pick them up and walk out the back entrance. With this method, they conducted a number of successful thefts in the business parks in the area. In the case of the company, they stole two laptops and a number of valuable personal items left on desks.

Unfortunately, by the time the thefts were discovered the criminals had already moved on. Upon reviewing the company's security procedures, the company realised that their security measures failed to take into account the planning and initiative of malicious actors.

What can you do to mitigate this situation?

- Encourage staff to "challenge" any person they do not know. This could include questioning pass wearers who are not from the normal work area unless they are accompanied by known staff.
- Have single-person entry sliding panels that can be readily observed and consider pass controlled doors for certain levels of security classification.
- Have RFID detectors for passes that are coded for particular areas and triggers an alert if there is unauthorised access.
- Install video surveillance for entries and key areas.
- Install biometric access to sensitive areas.
- Test access vulnerabilities using a "red team" approach.
- As a workplace practice, periodically adjust site use habits and routines.


307
ARMY

Chapter 7: DISP ICT and cyber security requirements

1. About DISP ICT and cyber security

ICT and cyber security involve the identification of, protection from, and remediation of security incidents or attacks on your ICT systems and digital networks.

By becoming an Entry Level DISP member and implementing the controls required for membership, you are demonstrating your commitment to being proactive in protecting information, assets and people. Understanding the real risk of a cyber incident and the counter measures you can put in place will only improve the outcomes for your business. It is not about doing the bare minimum to meet the criteria for DISP membership but improving your posture against the probability of a cyber attack.

2. Determining the right DISP level

Membership level	ICT and cyber security requirements
Entry Level	Entry Level ICT and cyber security requires self-certification against your chosen cyber security maturity model. You can self-certify by completing the DISP membership form and nominating which cyber security standard that your business meets.
Level 1	Entity has, or requires, at least one network or standalone device to store, process and communicate up to PROTECTED information.
Level 2	Entity has, or requires, at least one network or standalone device to store, process and communicate up to SECRET information.
Level 3	Entity has, or requires, at least one network or standalone device to store, process and communicate up to TOP SECRET information.

3. DISP levels for ICT and cyber security requirements

To meet appropriate levels for ICT and cyber security requirements, you will need to:

- determine which cyber security standard is right for your business;
- participate in the DISP Cyber Security Assurance Process;
- assess your systems and networks;
- implement your chosen standard; and
- provide evidence your business meets the required standard (at Entry Level this means self-certification through completion of the DISP membership form).

3.1 Determine which cyber security standard is right for your business

There are four cyber security standards you can choose from depending on your business and contractual needs:

1. ASD Essential 8 (Top 4)
2. NIST SP 800-171
3. Def Stan 05-138
4. ISO/IEC 27001 and 27002

The below table compares the four cyber security standards:

ASD Essential 8 (Top 4) Australian standard	• Your business needs to meet the Top 4 of the Essential 8 to meet DISP ICT and cyber security requirements • The Top 4 are: application control, patching applications, patching operating system vulnerabilities, and restricting administrative privileges • This is often the standard used for Australian businesses operating in the Australian environment
NIST SP 800-171 US standard	• Potentially a good option for businesses currently or intending to operate within the US or with US stakeholders (including exporting to the US) • Mandatory for businesses with a contractual obligation to meet the standard
Def Stan 05-138 UK standard	• Available for businesses who have a contractual obligation to meet the standard, present under an old policy arrangement
ISO/IEC 27001 and 27002 International standard	• Internationally recognised standards • Conducts its own accreditation and auditing activities • Potentially a good option for businesses currently or intending to work in multiple countries (including exporting to multiple countries) • Appropriate for the purposes of meeting DISP membership requirements. For specific applications, it is recommended that businesses also review additional standards under the ISO/IEC 27000 family of standards.

INDUSTRY TIP

Role of the Chief Information Security Officer (CISO)

In the context of cyber security, it is becoming more common for organisations to include the CISO as part of its executive team. They are responsible for information and data security, which may encompass, complement or support the roles of the CSO, head of security, CIO and head of IT (depending on the organisation).

It is now becoming more common, however, for the CISO to be accountable for both technical and non-technical areas within a business. According to the 2019 CISO Lens Benchmark report, the CISO's potentially wide-ranging role may extend to responsibilities involving "privacy, business continuity, crisis management, disaster recovery and internal/external fraud".

As the Benchmark report notes there is "no one size fits all" for the role of the CISO and their reporting lines. For the purposes of DISP membership, it will be important for DISP members to understand the role of the CISO and their obligations to meet the relevant level and category of DISP membership.

Sources: https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html; https://www.cisolens.com/benchmark.

3.2 DISP Cyber Security Assurance Process

The Defence Industry Security Office (DISO) has developed a contemporary audit and assurance program focused on providing Defence confidence that DISP members are meeting their security requirements and are mitigating the most pressing security risks that we collectively face. As part of the program, Defence is conducting more audits and seeking more information on the security posture from DISP members and applicants.

This activity includes the DISP cyber security assurance process which captures the necessary information for DISO to better understand the cyber maturity of DISP members and applicants. This information enables DISO to focus more effectively on how they can assist DISP members and applicants to uplift their security posture and resilience.

The DISP Cyber Security Assurance Process comprises the following:

- **Point of entry assessment:** Industry is not granted DISP membership unless they can demonstrate that they have in place security standards for the level which they have nominated. This includes the completion of a cyber maturity questionnaire which captures DISP members' and applicants' current cyber security posture and provides the detail required to derive a maturity assessment based on the ASD's Essential 8 Mitigation Strategies. The completed assessment will be reviewed by DISO to identify relevant gaps and provide remediation recommendations to support uplift.

- **Ongoing assurance:** Once in the DISP, industry partners are subject to ongoing assurance activities including on-site security audits. The on-site audits offer a more reliable source of information to assess the cyber security maturity. DISO cyber auditors will assess ICT governance frameworks and policies (sighting and inspecting artefacts) as well as the physical controls surrounding ICT systems and server rooms. Interviews with the Chief Information Security Officer and system administration staff will also be conducted.

DISO cyber security audit approach

To gain a holistic understanding of a member's cyber maturity, DISO cyber audits will follow the cyber security principles described in the ISM.

ISM Cyber Security Principles	DISO Cyber Security Audit Approach
Govern: Identifying and managing security risks	DISO will assess and interpret the governance documents that support the network
Protect: Implementing security controls to reduce security risks	DISO will assess the technical controls to determine the level of cyber maturity
Detect: Detecting and understanding cyber security events	DISO will determine whether a member has in place detection and prevention polices
Respond: Responding to and recovering from cyber security incidents	DISO will determine the members' understanding of reporting and responding to a cyber incident

Technical solutions

Given the expected growth of the DISP membership, it is not practicable or feasible to undertake face to face cyber audits of all DISP members, and while desktop audits provide an understanding of a DISP member's cyber security, anecdotally self-attestation is at the lower end of assurance. Therefore, a technical solution, which involves a downloadable agent (tool) by the organisation will enable DISO to understand cyber maturity standards at a much greater scale. DISO is currently piloting this technical solution.

NOTE

The tool, a downloadable agent, gathers data over a chosen period (seven days), providing a dashboard view of an organisation's compliance with the ASD Essential 8 controls, however the focus will be the 'Top 4' as specified in the DSPF. The dashboard view will be configured to be aligned with the DISO Cyber Maturity Model, providing accurate data of an organisation's Entry Level systems and networks. Collectively, this data can be used by the organisation to self-identify opportunities for improvement, in order to improve their cyber maturity. Further, the tool can be used to follow up with organisations to ensure that opportunities for improvement or recommendations have been implemented.

3.3 Assess your systems and networks

Assessing your systems and networks will help you determine how and where to apply your chosen cyber security standard.

To do this, you will need to:

1. Understand which of your systems and networks must meet the standards, including:

- The systems and networks owned by your business.
- The systems and networks that will be storing, processing or communicating Defence information, including cloud services or systems owned, managed or controlled by parties other than your business.

2. Determine any gaps you need to address to meet your chosen standard.

To assess your current systems and networks, you may need to seek advice from an IT service provider.

Another important and recommended resource for you to understand is the Australian Government's Information Security Manual (ISM). The purpose of the ISM is to outline a cyber security framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats. Many of the principles in the ISM will help guide you in cyber matters: https://www.cyber.gov.au/acsc/view-all-content/ism.

INDUSTRY TIP

Customer and Defence transactions security

An SME's critical asset is their customer information, which becomes even more important when working with Defence. This information may be managed in the SME's customer-transaction database, which includes order history, contact information and other commercial information. It may have taken many years of staff effort to establish customer relationships, loyalty and trust, and this information needs to be properly protected. Associated costs include set up costs to establish a database system to manage this critical information. Ongoing operations and maintenance costs include measures to protect this information and these investments should be undertaken annually.

There are various security risks associated with handling of customer information in databases, which requires specific responses to manage and prevent specific events, impacts, and consequences. Sources of risk include:

- Competitors, security breach perpetrators and insider threats may regularly attempt to obtain access to, or a copy of, this information (high risk).
- Sales and marketing staff may be approached by competitors to disclose this information for personal financial gain (medium risk).
- Third party attackers may threaten to obtain access to and disclose this information on the internet (low risk).

How would you quantify the "risk" to your organisation if a breach of your customer-transaction database occurs and how do you assess your risk tolerances? What would be the appropriate measures to protect your information?

What can you do to mitigate this risk?

- Security requirements for the customer-transaction database might include zero tolerance of unauthorised disclosure (violation of confidentiality), continuous validation of data integrity (by automated comparison with a trusted, securely stored version), and 99.999 per cent availability (risk tolerances).
- Implement policies and procedures that state these requirements and risk tolerances for this asset.

- Clear assignment of roles and responsibilities and periodic training for staff and managers involved in protecting this asset.
- Periodic training for staff having access to this asset.
- Immediate removal of access and authorisation for any staff member whose responsibilities no longer require a need for access, including any change in employment status such as termination.
- Infrastructure architecture that fulfils these requirements, meets these risk tolerances, and implements effective controls e.g. strong authentication, firewalls including ingress and egress filtering, enforcement of separation of duties, automated integrity checking, hot backups, etc.
- Review of all new and upgraded technologies that provide database support and in-house and remote access to determine if any of these technologies introduce additional security risks or reduce existing risks. Review occurs before and after technology deployment.
- Regular review and monitoring of relevant processes, and performance indicators and measures including financial performance and return on investment.
- Regular review of new and emerging threats and evaluation of levels of risk.
- Purchasing cyber insurance.
- Regular audit of relevant controls and timely resolution of audit findings.

3.4 Implement your chosen standard

You will need to apply your chosen security standard to any systems or networks that will be involved in storing, processing or communicating Defence information.

You can find information on implementing your chosen cyber security standard using the following links:

- ASD Essential 8 (Top 4): https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-explained
- NIST SP 800-171: https://csrc.nist.gov/publications/sp800
- Def Stan 05-138: https://www.gov.uk/government/publications/cyber-security-for-defence-suppliers-def-stan-05-138
- ISO/IEC 27001 and 27002: https://www.iso.org/standard/54534.html and https://www.iso.org/standard/54533.html

More information on implementing the ASD Essential 8 (Top 4)

The ASD Essential 8 (Top 4) is a common cyber security standard and important to understand for Entry Level DISP membership and above:

1. ***Application control*** – A security approach designed to protect against malicious code (also known as malware) executing on systems. When implemented properly it ensures that only authorised applications (for example, executables, software libraries, scripts and installers) can be executed.
2. ***Patching applications*** – Applying patches (patching software released by a vendor) to fix an issue with authorised applications (for example, executables, software libraries, scripts and installers).
3. ***Patching operating system vulnerabilities*** – Applying patches (patching software released by a vendor) to fix an issue relating to an operating system.

4. ***Restricting administrative privileges*** – Determining what tasks should only be completed by those with administrative privileges and creating separate accounts for staff who will need to complete these tasks as part of their duties.

Note on cloud services

Many businesses might use services, for example, to store data that are located offsite and offshore including cloud services. If you use cloud services or have third party systems there are additional issues to consider in meeting the ASD Essential 8 (Top 4) requirements. If you are in a contract with Defence which involves storing and using sensitive and classified information, DSPF Principle 21 and Control 21.1 addresses the scenario of offshore and cloud based computing, and you should refer to these in addition to Control 15.1 Foreign Release of Official Information which require approvals if information is available for foreign nationals or countries to access.

Separately, if your business has information that does not relate to Defence work, it is your business's decision whether to use offshore and cloud-based services for non-Defence related information. In addition, the technical advice in this space changes regularly and requires specialist knowledge so we recommend you consult with an ICT professional.

Visit the ACSC website for practical advice on how to implement the ASD Essential 8 (Top 4) for Windows and Linux: https://www.cyber.gov.au.

NOTE

You may choose to use an IT service provider to certify your systems and networks meet the requirements of your chosen cyber security standard. Some questions you might ask in determining the right IT service provider are in the case study below.

CASE STUDY

Ransomware attack

A small to medium-sized company was in the middle of delivering a major contract with a Government agency.

When its Vice President logged onto their computer on Monday, they discovered that all the files on their server were encrypted with an unknown file type. When they attempted to open any file, they were alerted with an error message on their server saying the file could not be opened.

They called their IT service provider to investigate it. It was found the server was hit by a ransomware attack and a message was left demanding payment before the files could be unlocked. Sensitive government information may have also been exfiltrated by the actor prior to the extortion attempt via ransomware.

Upon investigation, it was realised that – luckily – their on-site backups were not compromised by the cyber-attack and were accessible.

In the meantime, their production was stalled while they were returning their systems back online via their backups. Without these backups, the business would have faced significant delays in returning to normal operations and there was a real possibility that jobs would have been lost as a result. This was obviously a very stressful time for the business. Potentially this incident could have seriously affected their business and reputation.

When they reviewed their IT contract, it turned out that the contractor had not set up proper procedures when it came to their cyber security, which meant that their server was more vulnerable to a ransomware attack.

What can you do to mitigate this situation?

Consider asking your IT provider these questions:

- What previous work have you done with government agencies, particularly with Defence?
- What experience have you had in certifying industry members in cyber security standards, such as the Top 4 of the ASD Essential 8.
- What types of cyber attacks do you mitigate and how?
- What business continuity plans do we have (or should have) in place?
- How will you protect the critical parts of our data and systems?
- How do we satisfy ourselves that the backup is working properly and we are backing up the right information?
- What do you do to ensure the backups are working as designed and the system is secure?
- How are backups protected? Are they encrypted? How often are they occurring?
- What custom-made applications are you using and how could these risk our business?
- In the event of our server being locked down, how would you get us up and running again?
- How long would this take?
- Could you change the way we are setup to improve this?

Additional tips:

- Such cyber security incidents should be reported – see Chapter 10 for further information.
- If you are using an external service provider for your ICT needs, you need to ensure that this service complies with your Export Import obligations such as ITAR agreements and licences.

Auditing of your systems and networks

Your systems and networks may be audited by Defence at any time to ensure they meet the cyber security standard stated in your certification documentation.

INDUSTRY TIP

If you use Office 365, to ensure you meet your security requirements you will need to reconfigure the settings, rather than relying on the standard settings. You may have specific needs for your business so you should contact your IT service provider to make sure it is configured right for you.

INDUSTRY TIP

Cyber insurance

Most, if not all, Defence related contracts – particularly those which have any connection with the US – must have cyber insurance protection.

Ensure the organisation has sufficient cyber security insurance coverage:

- Policies are graded relative to the size of the business;
- Check the policy as to what it does and, most importantly, does not cover; and
- Seek specialist advice.

Finally, if cyber insurance is a requirement in certain Defence contracts, companies should consider what services their cyber insurance provides and how these will work in a cyber security incident, or how they improve their organisation's cyber security maturity. Organisations can refer to the ACSC for the latest information/advice.

INDUSTRY TIP

Data breach from compromised software

Data breaches arising from compromised software is not an uncommon scenario. Ensuring there are no vulnerabilities in the software used by a business may be outside of the control of end user companies. However, businesses can still mitigate the impact of this situation:

- Companies should patch their software as a top priority (ASD Essential 8 (Top 4)).
- Change any passwords, particularly admin from the default security passwords.
- Consider a password manager for all company staff.
- Add multi-factor authentication, if your provider has enabled it, and ask them why not if they have not. The method of authentication using a text message is not the most secure multi-factor authentication. You should consider your individual security requirements and choose the appropriate method. (Further best practice guidance on multi-factor authentication is available from the ACSC website: https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-multi-factor-authentication.)
- If you are using an external service provider for your IT/network security, you should pay more attention to how they are safeguarding your access and information, particularly remote access and administrative privileges required by them to support your business.

4. Advanced level ICT and cyber security requirements

Membership level	ICT and cyber security requirements

Level 1	• Have a self-certified corporate network meeting at least one of the following standards:
	  ○ ASD Essential 8 (Top 4)
	  ○ NIST SP 800-171
	  ○ Def Stan 05-138
	  ○ ISO/IEC 27001 and 27002
	• Have at least one network or standalone device to store, process and communicate up to PROTECTED information
	• Get Defence accreditation of your network or standalone device

Level 2	• Have a self-certified corporate network meeting at least one of the following standards:
	  ○ ASD Essential 8 (Top 4)
	  ○ NIST SP 800-171
	  ○ Def Stan 05-138
	  ○ ISO/IEC 27001 and 27002
	• Have at least one network or standalone device to store, process and communicate up to SECRET information
	• Get Defence accreditation of your network or standalone device

Level 3	• Have a self-certified corporate network meeting at least one of the following standards:
	  ○ ASD Essential 8 (Top 4)
	  ○ NIST SP 800-171
	  ○ Def Stan 05-138
	  ○ ISO/IEC 27001 and 27002
	• Have at least one network or standalone device to store, process and communicate up to TOP SECRET information
	• Get Defence accreditation of your network or standalone device

To meet higher level (Level 1, Level 2 and Level 3) ICT and cyber security requirements, you will need to:

1. Determine which advanced DISP level you need
2. Meet ICT and cyber security requirements for Entry Level
3. Determine the best way to meet advanced level requirements
4. Implement your chosen option
5. Get Defence accreditation of your network or standalone device

4.1 Determine which advanced DISP level you need

Determine what level of Defence information you will need to store, process or communicate in your business. The advanced levels are:

- **Level 1** – up to PROTECTED information
- **Level 2** – up to SECRET information
- **Level 3** – up to TOP SECRET information

4.2 Meet ICT and cyber security requirements for entry level

An Entry Level membership means your business has a self-certified corporate network meeting at least on the following standards as described above:

- ASD Essential 8 (Top 4)
- NIST SP 800-171
- Def Stan 05-138
- ISO/IEC 27001 and 27002

4.3 Options to speed up the certification and accreditation process for higher levels

If you aspire to meet DISP membership Level 1 or above, you can apply for a higher level of membership. As part of the application process, your business can undergo the accreditation process.

There are different ways your business can meet advanced level requirements depending on whether:

- You want to proactively meet advanced level requirements for future work with Defence; or
- You have a current contract with Defence and need to meet an advanced level.

Options to meet advanced level membership requirements are:

- **Option 1** – Get an IRAP assessment. However, note that this is an expensive process, and may not be feasible for many companies due to costs.
- **Option 2** – Use a standalone device. Even standalone systems at the classified level need to be appropriately approved by Defence for storage and processing of classified information via the CIOG ICT Security Branch.
- **Option 3** – Use a Defence network or device i.e. DREAMS token (DPN), or physical install of DPN, DSN or TSN terminal. This option is only available to current Defence contract holders with a legitimate need. This solution is arranged by your Defence contract manager on a case-to-case basis.

Pros and cons of each option

Option	Pros	Cons
Option 1 – Get an IRAP assessment	✓ May expedite DISP membership process	× IRAP security assessments can be a prohibitively expensive option × Defence accreditation still required

Option	Pros	Cons
Option 2 – Use a standalone device	✓ Cost effective option	× May not be suitable for your business × Defence accreditation still required
Option 3 – Use a Defence network or device	✓ Cost effective option ✓ Defence ICT accreditation not required	× At the discretion of the Defence contract or project manager

We recommend contacting Defence via yourcustomer.service@defence.gov.au to discuss the best option for your business before making a decision.

4.4 Implement the chosen option

Implement the best option for your business depending on your business needs.

Option 1 – Get an IRAP assessment

For this option you will need to get an IRAP security assessment by an IRAP Assessor to ensure your network meets requirement: https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-assessors.

Option 2 – Use a standalone device

For this option you will need to:

1. Get a standalone device (i.e. not connected to a network) able to store information up to your desired level (e.g. a PROTECTED laptop);
2. Demonstrate how you will apply physical security measures to protect the device up to your desired level (e.g. a device stored in a PROTECTED storage unit); and
3. Demonstrate how you will get information on and off your standalone device (e.g. using a USB to get information onto your advice or using a standalone printer to print from the device).

To set up a standalone device that meets the requirements, you may need to seek advice from an IT service provider.

Classified laptops/standalone systems are normally required to be approved/accredited by the CIOG ICT Security Branch.

Option 3 – Use a Defence network or device

If you are already working on a Defence contract, your Defence contract manager or project manager may agree to give your business access to a Defence system (e.g. DPN, DSN or TSN) or device (e.g. Defence laptop or DREAMS token).

You do not need to get Defence accreditation if this option is available to your business. Physical accreditation will still occur as you will require a suitably secure area to house the devices.

NOTE

Any person with DPN login may request a DREAMS virtual/physical token to allow DREAMS access.

4.5 Get Defence accreditation of your network or standalone device

You will need to get Defence accreditation that your network or standalone device can store, handle and communicate Defence information for your desired level. You will need to get Defence accreditation for:

- **Option 1** – Get an IRAP assessment.
- **Option 2** – Use a standalone device.

The Defence accreditation process has no additional cost to business, however can take a considerable length of time to complete.

To get accreditation of your network or standalone device, apply for the required level of ICT and cyber security membership accordingly through your AE250 application form.

You will be assigned a CIOG consultant who will get in contact with you within 10-20 business days to provide Defence accreditation.

5. Costs and timeframes and frequently asked questions for ICT and cyber security

5.1 Costs and timeframes for implementing the standard

The cost and timeframes for implementing your chosen cyber security standard is dependent on:

- The current level of cyber maturity of your business, and what gaps you need to fill to meet the requirements.
- The size of your systems and networks.
- Complexity of your systems and networks, such as access and connectivity to cloud services, external service providers or third party infrastructure.
- Your number of employees.

Note: Further information about likely costs for initial DISP membership is discussed in Chapter 2.

5.2 Costs for maintaining the standard

There will being ongoing costs to maintain your chosen cyber security standard.

You may choose to use an IT service provider to ensure your networks and systems continue to meet cyber security requirements.

INDUSTRY TIP

Protecting security cameras

If you use security cameras or web cameras for your business, the following precautions should be given to mitigate them from being compromised:

- Change any passwords, particularly admin from the default security passwords.
- Add multi-factor authentication, if your provider has enabled it, and ask them why not if they have not. The method of authentication using a text message is not the most secure multi-factor authentication. You should consider your individual security requirements and choose the appropriate method.
- If you are using an external service provider for your camera security, you should pay more attention to how they are safeguarding your access and information.
- Consider additional protection of remote camera access via network segregation and/or use of VPN technologies.

INDUSTRY TIP

Protecting websites

Websites have been known to become compromised if they are not sufficiently protected. Consider asking your website host/provider these questions:

- What previous work have you done with government agencies, particularly with Defence?
- What types of cyber attacks do you mitigate and how?
- How will the critical parts of your data and systems be protected if your website is compromised?
- What custom-made applications are you using via the website and how could these risk your business?
- How often does the website and web application get penetration tested?
- Could your provider change the way you are setup to improve this?

If you are using an external service provider for your website needs, you need to ensure that this service complies with your Export Import obligations such as ITAR agreements and licences.

5.3 What is the difference between certified, self-certified and accredited and when do I need them?

Certification is when you identify, assess and report on the risk that your system presents to the information environment. Certification by a third party is official recognition that your system meets a particular standard.

For Entry Level membership you may *self-certify*, which means that you sign a form that you have assessed your system against the particular standard.

Accreditation is when an authoritative body (Accreditation Authority) gives formal recognition, approval and acceptance of the risk identified.

The CIOG is the Defence authority for accrediting systems (Defence and Defence industry) to hold classified information (up to SECRET).

Self-certification is only relevant at DISP Entry Level for ICT and cyber security. For Level 1 and above, accreditation of an ICT solution (either your own network, standalone device, Defence terminal installation,

or DREAMS token) is undertaken. The DISP team task the CIOG to verify existing accreditation or undertake new accreditation.

5.4 Do I need to get my systems and networks accredited for entry level membership?

No, you do not need to get your systems and networks accredited to meet Entry Level DISP membership requirements. At the time of application, applicants are not required to demonstrate certification by providing any additional documentation. It is only if a company is audited by the DS&VS that they will be asked to demonstrate the work undertaken to get their networks to the appropriate standard for which they declared they were compliant.

5.5 Do I need an IRAP assessment for entry level DISP membership?

No, you do not need to get for an IRAP assessment for Entry Level membership, however it can be useful for Level 1 and above in accelerating the accreditation process.

INDUSTRY TIP

IRAP costs

As a rough estimate, it has been suggested that gap assessments, reviews of System Security Plans, Threat and Risk Assessments, and Security Risk Management Plans will take a minimum 30-60 days, and will typically be billed at $1,200 per day (minimum).

To gauge the current rates for undertaking an IRAP assessment, search “IRAP” under Contract Notices on the AusTender website: https://www.tenders.gov.au/cn/search. From 2018 onwards, the contract value of IRAP services ranged between $20K and $270K. It is important to note that the value will likely vary according to the type and scope of services being sought.

For small and medium-sized businesses, it is important to consider whether the costs and services for IRAP are within their financial capacity versus whether the IRAP option is an easier path.

6. ICT and cyber security help and assistance

6.1 Australian Cyber Security Centre (ACSC) support

To get technical advice on meeting the ASD Essential 8 (Top 4) cyber security requirements, contact the ACSC on:

- Website: https://www.cyber.gov.au
- Email: asd.assist@defence.gov.au

In addition to the ASD Essential 8 (Top 4), the ACSC also offers the following which are available via its website:

- Supports businesses affected by cyber security incidents including providing assistance on managing incidents and receiving reports on cybercrime. See Chapter 10 below for further details.
- Provides news updates on cyber security incidents.
- Provides the latest advice for businesses in relation to mitigating and responding to cyber security incidents and threats.
- Offers a range of programs for managing cyber security.
- Responsible for the ISM.

The Commonwealth has also expressed strong expectations that defence industry will focus on meeting and exceeding cyber security requirements. You can sign up to the ACSC partner program here: https://www.cyber.gov.au/partner-hub/become-a-partner#no-back.

6.2 Cyber security risk tool

The Department of Industry, Science, Energy and Resources has made publicly available a Cyber Security Risk Tool which can be used by businesses to determine if they are likely to be a target for cyber attacks and also assess the level of maturity in their business cyber security practices. This tool requires the user to answer a 20-minute questionnaire and, based on the response, produces a tailored cyber assessment report about the business's overall cyber risk, with links to recommended resources and Business Advisers (if applicable). This tool can be accessed here: https://www.business.gov.au/cdic/build-your-business-in-defence/cyber-security-resources-for-defence-industry.

6.3 Secure cloud services

The ASD previously certified a range of cloud services that enable handling of information at particular levels of security classification. However, after 30 June 2020 the ASD ceased certification of cloud services.

To support secure adoption of cloud services across government and industry, the ACSC has released guides on its website for organisations to undertake the appropriate security assessments in relation to cloud services: https://www.cyber.gov.au/acsc/government/cloud-security-guidance. These are:

- Anatomy of a cloud assessment and authorisation: https://www.cyber.gov.au/acsc/view-all-content/publications/anatomy-cloud-assessment-and-authorisation
- Cloud security assessment report template: https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-security-assessment-report-template
- Cloud security controls matrix: https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-security-controls-matrix
- Cloud assessment and authorisation framework – frequently asked questions: https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-assessment-and-authorisation-frequently-asked-questions
- Cloud computing security considerations: https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-considerations
- Cloud computing security considerations for cloud service providers: https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-cloud-service-providers
- Cloud computing security considerations for tenants: https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-tenants

A practical application of appropriately secure cloud services is for the purposes of digital collaboration and networking between Defence and industry partners, both locally and overseas, which require handling of certain classified information. For example, GovTEAMS is a platform supported by the Department of Finance that is run on a previously ASD-certified cloud service that enables for this type of collaboration.[9]

Whichever cloud service tool is used, it is important for the business to understand the security capabilities and limitations of these services. For instance, GovTEAMS cannot be used for Export Controlled information. It is noted that GovTEAMS might be more useful for agencies not undertaking national security work. The acceptability of GovTEAMS is up to each Government agency and based on risk in relation to classified work. The system has been IRAP assessed and accredited to hold information up to and including the OFFICIAL: Sensitive classification, with a PROTECTED GovTEAMS currently being trialled.

[9] See https://www.govteams.gov.au.

Chapter 8: Ongoing obligations, audit and completion of DISP membership

1. Ongoing obligations and suitability for DISP membership

The DSPF Control 16.1 sets out the ongoing suitability requirements of DISP members. DISP members must:

a. safeguard Defence and industry's people, information and assets;

b. comply with the DSPF, including where applicable its referenced authoritative documents such as the ISM and relevant Defence policies covering physical, personnel and communication security policies and practices. Where the DSPF does not specify a policy position, industry should refer to the PSPF for guidance;

c. appoint and retain a CSO, and trained SO (the CSO and SO can be the same individual);

d. report any changes that may affect your DISP membership in accordance with the relevant requirements of the DSPF, including but not limited to:
   (1) eligibility and suitability changes;
   (2) FOCI changes;
   (3) security and fraud incidents (See DSPF Principle 77 – Security Incidents and Investigations);
   (4) contact with foreign officials; and
   (5) changes in circumstances for their security cleared personnel (e.g. contact details, relationship status, financial changes, overseas travel. See DSPF Control 40.1 – Personnel Security Clearances);

e. comply with all audit and assurance activities at the direction of the DS&VS, including completion of the Annual Security Report (ASR) every 12 months from the date of DISP membership; and

f. keep a register of overseas travel and travel briefings, and make it available to Defence upon request.

2. Participation in audit and assurance activities conducted by the Defence Industry Security Office

The DSPF also notes that to ensure compliance with the DISP minimum security requirements, Defence will:

a. undertake assurance and compliance activities;

b. review DISP member's ASR annually;

c. conduct random and targeted security checks of DISP members. This may include, but not limited to, a review of the company's security policies and plans, personnel, information and physical security arrangements and security registers, including physical security inspections;

d. assess industry security incident, fraud and contact reports, in accordance with DSPF; and

e. conduct security investigations as appropriate, in accordance with DSPF.

DISP assurance activities will also inform the Capability Acquisition and Sustainment Group (CASG) Company Performance ScoreCard rating.

DISO audit and assurance activities

By becoming a DISP member, you have a responsibility and agree to participate in the Defence Industry Security Office (DISO) audit and assurance activities.

DISO will undertake audits and other assurance activities of DISP members measuring compliance against the standards listed in the DSPF Control 16.1 and authoritative documents such as the ISM and PSPF.

Audits will be undertaken by Defence with support of contracted auditors and conducted in line with industry standards and better practice audit methodologies across the audit lifecycle (i.e. planning, fieldwork and reporting). This includes interviews with SOs and sighting relevant documents.

DISO's audit and assurance program consists of:

- Comprehensive audits that measure security maturity across all four domains of governance, personnel, physical, and ICT and cyber security;
- Sampling Assessments that measure the security maturity across DISP Entry Level requirements;
- Cyber Audits which will focus on the cyber maturity of your organisation; and
- Follow-up Reviews to ensure remediation from audits have been completed.

If you are selected to participate in an audit or assurance activity, depending on the scope and approach of the activity, you will receive formal notification of when the audit is to take place. DISO will provide an audit plan outlining the scope and approach, what to expect from fieldwork, information on the audit team and what is entailed in the reporting process. Depending on the audit findings, you may be required to develop a management action plan (map) outlining any remediation activities, including who will be responsible and timeframes for completion.

DISO audits add value for Defence and industry by identifying opportunities for improvement, the causes of any deficiencies, and any corrective actions needed. The intent of the audit is to assist the DISP member to uplift security. DISO will also provide general themes observed during its audits to industry to enable broader awareness and assist in uplifting overall security practices.

3. Upgrading or downgrading membership

A DISP member may apply to upgrade or downgrade their membership level for specific elements of the DISP, as appropriate for their business requirements, or in order to meet contractual requirements.

4. Ceasing DISP membership

According to the DSPF, DISP membership will continue until such time as it is voluntarily ceased by the DISP entity, or modified by Defence as a result of non-compliance.

Voluntary withdrawal or ceasing

Industry entities can voluntarily withdraw from the DISP application process at any stage or cease their membership by notifying Defence via email to DISP.submit@defence.gov.au.

Upon withdrawal or ceasing, Defence will notify all relevant parties in accordance with its Privacy Notice.

Membership Modification

Non-compliance with DISP membership requirements may result in Defence terminating, downgrading, limiting or suspending an entity's DISP membership.

Failure to comply with DISP membership requirements may also have other consequences, for example:

a. contractual penalties where obligations to meet a contractual requirement are not met; or

b. criminal or financial penalties or sanctions under Australian law.

Obligations and consequences

When DISP membership ceases:

a. where applicable, any sensitive or classified information or materials belonging to a project or program must be returned or destroyed in accordance with the contract terms and conditions;

b. the CSO and nominated SO's security clearances that were obtained for the purposes of DISP membership will cease to be sponsored by DS&VS and become inactive;

c. all the DISP member's personnel security clearances will also become inactive unless sponsorship is assumed by multiple interested parties;

d. facility and ICT system accreditation will lapse; and

e. Defence will notify affected parties (i.e. those that are related to a contracted project or program) of ceased memberships.

Chapter 9: Working in a defence industry supply chain

As noted, this Guide is focussed on the requirements for DISP membership. Many companies, however, will also need to work with a large contractor as part of a Defence industry supply chain. These large companies will have their own security requirements and it is important that companies understand these expectations, which will complement the DISP requirements.

1. How do I engage with larger companies and their supply chains?

If you are a small to medium-sized enterprise working in the Defence industry, or wanting to enter into a Defence industry supply chain, there are a range of things you can do to get started:

- Contact the CDIC to obtain advice on your business and your ability to provide Defence products and services. Website: https://www.business.gov.au/CDIC.
- Make sure you are registered with the appropriate Industry Capability Network (ICN) organisation in your State or Territory. Website: https://icn.org.au/.
- Review and make contact through the larger companies' websites and notify of your interest to provide goods and/or services.
- Make sure you establish your connections through various means including industry associations such as Ai Group, Australian Industry and Defence Network (AIDN), Defence Teaming Centre (DTC), and Australian Defence Alliance – Victoria (ADA).

2. What are the larger company's requirements for security?

Each larger company will have its own unique requirements for security, as well as a broader range of supplier assessments depending on the company and nature of the business. In some cases, companies will have security including cyber security assessments to help ensure your company is ready for Defence business. Each of the large Defence contractors will have its own security department that can help set the expectations around security and guide you through their processes.

3. Some principles involved in working in a Defence industry supply chain

It is critical that large and smaller companies work together to help ensure security resilience of our Defence industry supply chains. Some principles to underpin this relationship include:

- **Flow down of contract requirements** – Due to the importance of security requirements, the Commonwealth places a contractual obligation on large contractors to ensure that certain security clauses are directly flowed down to all subcontractors. The flow down clauses require subcontractors to agree to cooperate with Commonwealth security checks and to provide written undertakings in respect of security or access to Commonwealth premises. The flow down also includes the requirement to comply with the Commonwealth's PSPF, DSPF and ISM, in addition to specific contractual security clauses recommended in these policies. More information on the

Commonwealth's Australian Standard for Defence Contracting (ASDEFCON) templates can be found here: https://www1.defence.gov.au/business-industry/procurement/contracting-templates/asdefcon-suite.

- **Contract clarity** – In the contract between the prime and the subcontractor, all security requirements should be included or referenced to an agreed document such as the aforementioned policies and a Security Classification and Categorisation Guide (SCCG) for the project.
- **Due diligence** – Both large contractor and subcontractor should conduct a comprehensive appraisal of the security of a prospective partner, especially to establish its level and capability to meet security obligations.
- **Cost allocation** – The cost of security controls should be borne by both parties as required to meet their contractual obligations to each other and to the DISP.
- **Security requirements** – The security controls must meet the Security Policy and SCCG elements for each party in relation to the area of subcontracted work.
- **Security risk assessment** – In addition to the requirements of the SCCG, all parties should undertake a security risk assessment to identify any additional requirements to protect sensitive and classified information, activities, technologies, intellectual property, people and assets.
- **Review and audit** – Large companies should reach agreement with subcontractors for the timing, assessment and terms of reference for security reviews and audits. Audit programs will largely be based on risk and security performance of the subcontractor. Reviews and audits may be conducted by Defence, other Commonwealth security agencies, prime contractors or third party external auditors.
- **Communications** – All parties share responsibility for ensuring there are clear lines of reporting on security issues and incidents, and coordinate any reporting to Defence as required in the contract and Defence and Commonwealth security policies.
- **Training** – Both large company and subcontractor should ensure that all staff are trained to the level required under the DISP. All parties have an obligation to ensure correct implementation of the SCCG and to seek clarity where needed from Defence.

Chapter 10: What to do in the event of a security incident

1. Security incidents

This chapter sets out information on security incidents and what to do if an incident occurs in your business.

The DSPF Control 77.1 sets out the definitions of a security incident and the detailed process for incident reporting:
https://www1.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL.pdf.

The DSPF defines a security incident as an occurrence which results, or may result, in negative consequences for the security of Defence.

A **minor** security incident is an accidental or unintentional action involving failure to observe protective security policy mandatory requirements or procedures within the DSPF. Examples include (but are not limited to):

- access passes or identification documents lost or left insecure; and
- security classified material not properly secured or stored.

A **major** security incident is any deliberate, negligent or reckless action that leads, or could lead, to the loss, damage, corruption or disclosure of OFFICIAL information or assets. Examples include:

- the loss of material classified PROTECTED or above, or significant quantities of material of a lower classification;
- actual or suspected hacking into any ICT system;
- compromise of security keys or combination locks;
- actual or attempted unauthorised access to an alarm system covering a secured area where security classified information is stored; and
- repeated incidents involving the same person or work area where the combination of the incidents warrants an investigation.

A **reportable major** security incident is any occurrence that requires reporting to ASIO as defined in the *ASIO Act 1979* (Cth), including espionage or suspected espionage.

An assessment of the harm resulting from a security incident should be used in conjunction with the definitions above to assist in determining whether the incident is a minor, major or reportable major security incident. More information is available in the DSPF.

2. What to do in the event of a security incident?

The diagram below sets out the process for responding to the identification or occurrence of a security incident.

REFERENCES: DSPF Control 77.1 – Security Incidents and Investigations; Fact Finding Reference "Good decision-making in Defence: A guide for decision-makers and those who brief them"

When a security incident occurs or is identified, you **must** undertake the following actions:

1. Report the security incident to the CSO and SO for internal management. Your business will:
    - Identify the security incident
    - Record the event on a security risk register
    - Conduct an internal security risk assessment to determine the business impact level
    - Come up with a strategy to prevent the incident from reoccurring
2. Submit an XP188 Security Incident Report or XP168 Report of Contact of Security Concern to the SIC, including:
    - Full circumstances and details of the incident
    - Details of actions taken to contain or mitigate and prevent recurrence of the incident
    - Risk assessment and damage assessment or degree of compromise resulting from the incident

3. Contacts for security incidents

The SIC, in Defence Security and Vetting Services division (DS&VS), is the area responsible for the assessment, referral and monitoring (as required) of security incident reports received from across Defence and Defence industry.

For advice and support, contact:
Defence Service Centre on 1800 DEFENCE;
Security Incident Centre (SIC): security.incidentcentre@defence.gov.au; or
Your regional State or Territory DS&VS Security Office.

If the security incident is cyber related:

- You should email the ACSC at asd.assist@defence.gov.au for assistance in managing your cyber security incident.
- If you have suffered a cybercrime, you should contact the ACSC to report that you have been a victim of cybercrime at https://www.cyber.gov.au/acsc/report.
- For urgent matters, call the Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371).

Appendices

Appendix 1: Glossary of terms and definitions

Acronym	Title	Definition
ACIC	Australian Critical Infrastructure Centre	Responsible for identifying and managing risks to Australia's critical infrastructure. Website: https://cicentre.gov.au.
ACSC	Australian Cyber Security Centre	Responsible for monitoring cyber threats in Australia and providing cyber security advice to individuals and businesses. Website: https://www.cyber.gov.au.
AGD	Attorney-General's Department	Amongst other things, responsible for managing protective security policy related to delivery of Government business via the PSPF. Website: https://www.protectivesecurity.gov.au/about/Pages/directive-security-government-business.aspx.
AGSVA	Australian Government Security Vetting Agency	Responsible for processing and granting security clearances for government agencies in Australia. Website: https://www1.defence.gov.au/security/clearances.
ADF	Australian Defence Force	Australian military comprising of the Air Force, Army and Navy. Website: https://www.defencejobs.gov.au/about-the-adf.
Ai Group	Australian Industry Group	The peak national industry association representing private sector businesses in Australia including in Defence, manufacturing, ICT, labour hire, construction, engineering, transport & logistics, mining services and civil airlines. Website: https://www.aigroup.com.au.
AIDN	Australian Industry & Defence Network	A peak national body supporting Australian small and medium-sized enterprise suppliers to Defence and Security related customers. Website: https://www.aidn.org.au.
AS	Australian Standard	National standards developed and administered by Standards Australia for application in Australia. Website: https://www.standards.org.au/standards-development/what-is-standard.

Acronym	Title	Definition
ASD	Australian Signals Directorate	Responsible for defending Australia's interests through foreign signals intelligence, cyber security and offensive cyber operations. Website: https://www.asd.gov.au.
ASIC	Australian Securities and Investments Commission	Responsible for regulating Australia's integrated corporate, markets, financial services and consumer credit. Website: https://www.asic.gov.au.
ASIO	Australian Security Intelligence Organisation	Responsible for protecting Australians and their interests from serious security threats. Website: https://www.asio.gov.au.
ASR	Annual Security Report	An annual declaration by the CSO that their business continues to meet the eligibility and suitability requirements of the DISP.
CDIC	Centre for Defence Industry Capability	Responsible for supporting Australian small and medium-sized businesses to enter or work in the Defence industry. Website: https://www.business.gov.au/CDIC.
CDR	Consumer Data Right	A Commonwealth Government data regulation regime aimed at providing consumers the right to safely access certain data about them held by businesses. Website: https://treasury.gov.au/consumer-data-right.
CIOG	Chief Information Officer Group	Responsible for leading the design, delivery and operation of the information, computing and communications infrastructure to support military operations. Website: https://www1.defence.gov.au/about/chief-information-officer-group.
CPR	Commonwealth Procurement Rules	The rules for all Commonwealth Government procurements that entities are required to follow.
CSO	Chief Security Officer	Responsible for, and has oversight of, governance relating to security risk and arrangements, and championing a security culture within the business.
Def Stan	UK Defence Standard	UK Defence standards developed and administered by Defence Standardization (Dstan) under the UK Ministry of Defence. Website: https://www.gov.uk/guidance/uk-defence-standardization.
DFARS	Defense Federal Acquisition Regulation Supplement	US Defense regulations relating to procurement of goods and services that the US Department of Defense officials and its contractors are required to follow. Website: https://www.acq.osd.mil/dpap/dars/about_dfarspgi.html.
DFAT	Department of Foreign Affairs and Trade	Responsible for foreign, trade and development policy advice to the Government. Website: https://www.dfat.gov.au/.

Acronym	Title	Definition
DISO	Defence Industry Security Office	An organisation within DS&VS and provides independent assurance that DISP members are meeting their membership obligations.
DISP	Defence Industry Security Program	A membership-based program for industry that sets minimum security requirements and safeguards to help secure Defence capability, Defence industry and the supply chain.
DLM	Dissemination Limiting Marker	Information classified as being subject to security related disclosure and access restrictions. This is an old classification which discontinued from 1 October 2020. Website: https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx.
DOSD	Defence Online Services Domain	An online gateway for Defence employees and external authorised users requiring Defence services to access specific applications online. Website: https://osd.defence.gov.au.
DPN	Defence PROTECTED Network	Previously called the Defence Restricted Network (DRN).
DS&VS	Defence Security & Vetting Service	Responsible for leading Defence's protective security initiatives including the AGSVA, DSM and DISP. Website: https://www1.defence.gov.au/security.
DSAP	Designated Security Assessed Position	Position within an organisation that requires access to a certain level of classified material and the personnel in such a position will require to have appropriate security clearance.
DSN	Defence SECRET Network	Defence's network used to handle up to SECRET information.
DSPF	Defence Security Principles Framework	Provides principles, controls and instructions to support Defence personnel and others contracting/working with Defence to manage security risks. Website: https://www1.defence.gov.au/sites/default/files/2020-12/DSPF-OFFICIAL.pdf.
DTC	Defence Teaming Centre	A national member organisation which includes prime defence contractors, small-to-medium enterprises, professional service providers and academic institutions that are involved in supplying and supporting Defence capability. Website: https://dtc.org.au.
EAC	Electronic Access Control	A security technology for allowing and preventing access to a physical area.
EU GDPR	European Union General Data	An EU data protection and privacy regulation relating to EU citizens. Website: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en.

Acronym	Title	Definition
	Protection Regulation	
FIRB	Foreign Investment Review Board	Responsible for advising the Treasurer and Government on Australia's Foreign Investment Policy and its administration. Website: https://firb.gov.au.
FOCI	Foreign Ownership, Control and Influence	The extent of control the entity is under from a foreign entity or entities.
GSA	General Security Agreement	Relates to commercial financial arrangements where the debtor provides some form of security to the creditor.
IEC	International Electrotechnical Commission	A not-for-profit, quasi-governmental organisation, comprised of experts and delegates from industry, government bodies, associations and academia, for the preparation and publication of international standards for all electrical, electronic and related technologies. Website: https://www.iec.ch.
IMM	Information Management Marker	Information identified by an entity as being subject to non-security related access and use restrictions. Website: https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx.
IRAP	Information Security Registered Assessors Program	Individuals from the private and public sectors endorsed to provide cyber security assessment services to Australian governments. Website: https://www.cyber.gov.au/acsc/view-all-content/programs/irap.
ISM	Information Security Manual	Outlines a cyber security framework that organisations can apply, using their risk management framework, to protect their systems and information from cyber threats. Website: https://www.cyber.gov.au/acsc/view-all-content/ism.
ISO	International Organization for Standardization	An independent, non-governmental international standards organisation comprised of national standards bodies. Website: https://www.iso.org/home.html.
ITAR	International Traffic in Arms Regulations	Regulates the export, re-export and retransfer of Defence articles, including hardware and technical data, where these articles are listed on the United States Munitions List (USML). Website: https://www.pmddtc.state.gov/ddtc_public?id=ddtc_public_portal_itar_landing.
MSP	Managed Service Provider	For the purposes of this guide, an MSP is a business that is engaged by organisations to manage their IT services and

Acronym	Title	Definition
		infrastructure, requiring remote access to their customer systems to deliver these services.
NDB	Notifiable Data Breaches	Data breaches that fall under the *Privacy Act 1988* (Cth), referred to as the NDB Scheme, which amended the Privacy Act and commenced operation in May 2018. Website: https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme/.
NIST	National Institute of Standards and Technology	A US agency with an objective to promote US innovation and industrial competitiveness. Website: https://www.nist.gov.
NV1	Negative Vetting Level 1	Security clearance level enabling personnel access to material classified up to SECRET.
NV2	Negative Vetting Level 2	Security clearance level enabling personnel access to material classified up to TOP SECRET.
PSC	Personnel Security Clearance	Required for access to classified material.
PSPF	Protective Security Policy Framework	Provides guidance to Australian Government entities on implementing protective security policy in security governance, personnel security, physical security and information security. Website: https://www.protectivesecurity.gov.au.
PSSA	Protective Security Self-Assessment	For ongoing suitability as a DISP member, this assessment is part of meeting Defence initiated compliance and assurance requirements.
SCEC	Security Construction Equipment Committee	Responsible for the evaluation of security equipment for use by Australian Government departments and agencies. Website: https://www.scec.gov.au.
SIA	Security of Information Agreement or Arrangement	A formal government-to-government information-sharing instrument for the exchange and reciprocal protection of classified information. Website: https://ext.defence.gov.au/security/industry-resources.
SO	Security Officer	Responsible for developing and implementing the SPP and acts on behalf of the CSO.
SPA	Security Protected Asset	An asset that requires protection from unauthorised access, sabotage, wilful damage, theft or disruption through a safe and secure physical environment.

Acronym	Title	Definition
SPP	Security Policies and Plans	Describe how businesses will achieve the DSPF requirements, while also guiding all personnel on their individual security responsibilities.
SR	Security Register	A system of security risk oversight and management.
SRA	Security Risk Assessment	As part of a business's overarching security risk management process, it helps to identify all areas of security threats and vulnerabilities and assess the associated potential impact.
SSO	Security Standing Order	Recommended best practice. Each DISP should have an overarching protocol with specific site/location/project SSOs encompassing appropriate instructions for the workforce.
UK NCSC	UK National Cyber Security Centre	Responsible for providing cyber security advice and support for private and public sectors, and general public in the UK. Website: https://www.ncsc.gov.uk.

Appendix 2: Useful templates and additional information

- Annex A: Important legislation and policies that guide Defence industry security
- Annex B: How does Defence classify information?
- Annex C: Subcontractor/supply chain security
- Annex D: Security risk assessment example
- Annex E.1: Personnel security assessment – recruitment and induction
- Annex E.2: Personnel security assessment – exit
- Annex F: Physical security assessment example
- Annex G: Further information about physical security zones
- Annex H: Additional physical security measure considerations

Appendix 3: Other useful resources and contacts

Defence Industry Security Program (DISP) website

The DISP website provides guidance to industry on DISP membership:

- DISP website: https://www1.defence.gov.au/security/industry
- DISP forms and templates, training material, and other DISP reference material: https://ext.defence.gov.au/security/industry-resources

Contract managers fact sheet

The Contract Managers Fact Sheet provides information on contract manager responsibilities relating to DISP.

- Contract Managers Fact Sheet: https://ext.defence.gov.au/sites/default/files/media/contract_managers_fact_sheet.pdf

Webforms

- AE250-1 – Foreign Ownership, Control and Influence: https://ext.defence.gov.au/security/industry-resources
- AE250-2 – Notification of Engagement Requiring DISP Membership: https://ext.defence.gov.au/security/industry-resources
- XP168 – Security Contact Concerns Report: https://www1.defence.gov.au/security/industry/make-security-report
- XP188 – Security Incident Report: https://www1.defence.gov.au/security/industry/make-security-report

Other resources

For further information, there are extensive sources with practical advice relating to security, including:[10]

- Attorney-General's Department:
  - Security governance for contracted goods and services providers: https://www.protectivesecurity.gov.au/governance/security-governance-for-contracted-service-providers/Pages/default.aspx
- Australian Critical Infrastructure Centre:
  - Protecting your critical infrastructure asset from foreign involvement risk: https://cicentre.gov.au/resources
- ACSC:
  - Anatomy of a Cloud Assessment and Authorisation: https://www.cyber.gov.au/acsc/view-all-content/publications/anatomy-cloud-assessment-and-authorisation
  - Cloud Security Assessment Report Template: https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-security-assessment-report-template
  - Cloud Security Controls Matrix: https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-security-controls-matrix
  - Cloud Assessment and Authorisation Framework – Frequently Asked Questions: https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-assessment-and-authorisation-frequently-asked-questions
  - Cloud Computing Security Considerations: https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-considerations
  - Cloud Computing Security for Tenants: https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-tenants

[10] https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management; https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management-practitioner-guide.

    - Cyber Supply Chain Risk Management: https://www.cyber.gov.au/acsc/view-all-content/publications/cyber-supply-chain-risk-management
    - Identifying Cyber Supply Chain Risks: https://www.cyber.gov.au/acsc/view-all-content/publications/identifying-cyber-supply-chain-risks
    - Guidelines for Outsourcing: https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-outsourcing
    - How to Manage Your Security When Engaging a Managed Service Provider: https://www.cyber.gov.au/acsc/view-all-content/publications/how-manage-your-security-when-engaging-managed-service-provider
    - Questions to ask Managed Service Providers: https://www.cyber.gov.au/acsc/view-all-content/publications/questions-ask-managed-service-providers
    - MSP Better Practice Principles: https://www.cyber.gov.au/acsc/view-all-content/programs/msp-partner-program-msp3
    - Strategies to Mitigate Cyber Security Incidents: https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents
- Department of Finance:
    - Commonwealth Procurement Rules: https://www.finance.gov.au/government/procurement/commonwealth-procurement-rules
- National Cyber Security Centre (UK):
    - Supply Chain Security Collection: https://www.ncsc.gov.uk/collection/supply-chain-security
- National Institute of Science and Technology:
    - Cyber supply chain risk management project website including best practices and standards: https://csrc.nist.gov/projects/cyber-supply-chain-risk-management

Australian Government

Department of Defence

Ai GROUP | DEFENCE COUNCIL