Australian Government
Defence

DISP

DEFENCE INDUSTRY SECURITY PROGRAM

APPLYING FOR DISP MEMBERSHIP

FAMILIARISE yourself with the program, framework and requirements

DETERMINE the level of membership you need

ASSESS your ability to meet the requirements and gather documents

COMPLETE the application in the DISP Members Portal

SUBMIT your application and understand what is next

For detailed information, refer to the How to Apply section of the DISP website.

Familiarise yourself with the program, framework and requirements

DISP supports industry to improve their security when engaging with Defence. It is a membership-based program that is a control from the Defence Security Principles Framework (DSPF) [PDF 10,220KB] in assuring that the Government's significant investment in Defence capability is appropriately protected.

The DSPF [PDF 10,220KB] is a principles-based framework intended to support a progressive protective security culture that understands and manages risk, leading to robust security outcomes. Principle 16 and Control 16.1, starting on page 145 of the DSPF [PDF 10,220KB] provide principles, controls and instructions to support Defence industry to understand and manage security risks.

DISP membership enables entities to improve their security operating environment, access Defence security services, training and materials, sponsor their own security clearances, broaden the range of contracts they can tender for and gain advice and analysis on the latest security trends and threats.

Note: your entity only needs one DISP membership regardless of the number of Defence contracts it holds.

To apply for DISP membership, your entity must:

- Be registered in Australia with an ABN.

For more information, refer to business.gov.au.

- Be financially solvent.
- Have a Chief Security Officer (CSO) and a Security Officer (SO) who meet the requirements set out in the CSO and SO Roles and Responsibilities Fact Sheet and are able to obtain a Digital Identity, such as myGovID, which is linked to your entity via Relationship Authorisation Manager (RAM).

For support with Digital Identity, please visit www.digitalidentity.gov.au/support.

- Have an established email address in the format of DISP@YourEntityName which is hosted in Australia.

For more information, refer to the How to Create a DISP@ Email Address Guide.

- Satisfy Defence requirements for Foreign Ownership, Control or Influence (FOCI) [PDF 645KB].
- Not have any relationships with a listed terrorist organisation, regimes subject to United Nations Security Council (UNSC) and Australian autonomous sanctions laws or persons and/or entities on the Department of Foreign Affairs and Trade's (DFAT's) Consolidated List.
- Have an ICT network that meets one of the following cyber security accreditation standards:
  - Top 4 of the Australian Signals Directorate (ASD) Essential 8
  - International Organization for Standardization (ISO/IEC) 27001 and 27002
  - U.S. National Institute of Standards and Technology (NIST) SP 800-171
  - UK Defence Standard (Def Stan) 05-138

Please ensure that you have read and understand the Eligibility and Suitability criteria on the DISP website and Principle 16 and Control 16.1 of the DSPF, starting on page 145 of the DSPF [PDF 10,220KB] prior to applying.

If you require support or have questions, please contact DISP.info@Defence.gov.au.

Determine the level of membership you need

There are four DISP Membership levels that align with Australian Government security classifications and four security domains. A membership level for each of the security domains must be selected based on your entity's requirements.

Security Domains:	Personnel Security	Physical Security	Information & Cyber Security	Governance
Questions to answer for membership level selection[1]:	Does your entity require the ability to sponsor and manage security clearances?	*Do you need to handle or store classified (PROTECTED or above) information physically on your company's premises?*[2]	*Do you need to handle or store classified (PROTECTED or above) information or assets on your company's ICT networks?*[2]	*What is the highest level you have selected across the other three domains?*
Entry Level	No, required security clearances will be sponsored by Defence or another government agency	No, my entity only handles or stores OFFICIAL / OFFICIAL: Sensitive information or assets	No, my entity ICT networks only handle or store OFFICIAL / OFFICIAL: Sensitive information	Entry Level (OFFICIAL / OFFICAL: Sensitive)
Level 1[1]	Yes, at the BASELINE (PROTECTED) level[3]	Yes, my entity requires at least one facility/room to be able to handle or store PROTECTED information or assets	Yes, my entity ICT networks require accreditation to handle or store PROTECTED information[2]	Level 1 (PROTECTED)
Level 2[1]	Yes, up to and including NV1 (SECRET) level[3]	Yes, my entity requires at least one facility/room to be able to handle or store SECRET information or assets	Yes, my entity ICT networks require accreditation to handle or store SECRET information[2]	Level 2 (SECRET)
Level 3[1]	Yes, up to and including NV2 (TOP SECRET) level[3,4]	Yes, my entity requires at least one facility/room to be able to handle or store TOP SECRET information or assets	Yes, my entity ICT networks require accreditation to handle or store TOP SECRET information[2]	Level 3 (TOP SECRET)

[1] Appropriate business case justification must be provided when applying for level 1, 2 or 3 membership; holding a Defence contract alone is not sufficient justification. A higher membership level requires more rigorous, complex and time-consuming application and assessment processes as well as greater governance and administration for the entity including higher costs for physical and ICT infrastructure and accreditation.

[2]Please select Entry Level membership for the Physical Security and Information and Cyber Security domain, unless you have existing certification and accreditation from Defence or an explicit requirement for a higher level to fulfil a current Defence contract.

[3]A DISP Security Officer must have a minimum NV1 clearance to sponsor clearances.

[4]DISP members cannot sponsor Positive Vetting (PV) security clearances; Defence SES Band 3 sponsorship is required to obtain a PV security clearance.

Note: Your membership level may be upgraded or downgraded as appropriate after it is initially granted.

For more information, including examples of entities and the levels for which they should apply, refer to the How to Apply section of the DISP website.

Assess your ability to meet the requirements and gather documents

The DISP Membership Requirements Checklist [PDF 188KB] is a key resource to help you answer the required questions prior to applying for DISP membership.

Please ensure that all information you provide about your entity matches the information recorded in the ASIC register, especially your registered business address and ABN/ACN.

Please ensure that you have gathered the following mandatory documentation to support your application:

- Applicant's Security Clearance level and status with CSID (your unique AGSVA ID found on myClearance or clearance emails from AGSVA) and date received, if applicable and Security Officer Training status with completion date and certificate, if applicable.

Note: you are able to proceed with your DISP membership application if you do not yet have a Security Clearance or have not yet completed Security Officer Training. However, membership will not be granted until your SO and CSO receive their clearances and attest to their intent to complete the training.

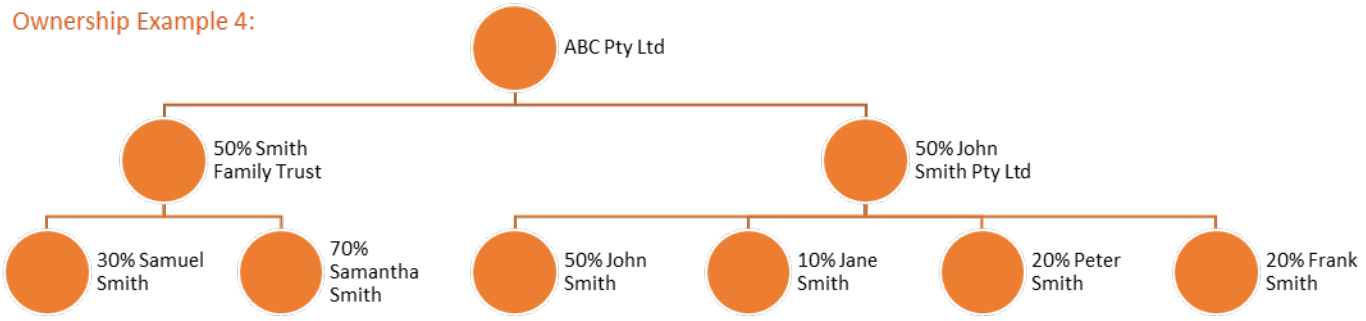
- A statement/list/chart/diagram that depicts the financial ownership of your entity, including all parent companies and their affiliates, ultimate beneficiaries, joint ventures, limited partnerships and subsidiaries.

Ownership Example 1: ABC Pty Ltd is solely owned by John Smith

Ownership Example 2: ABC Pty Ltd shareholding is 100% John Smith

Ownership Example 3: ABC Pty Ltd shareholding is 50% John Smith and 50% Jane Smith

Ownership Example 4:



Further documentation:

Further documentation, such as the following, may be required depending on the level of membership you are applying for and your answers to questions in the application:

- If you have a Defence contract which requires DISP membership, an AE250-2 form [PDF 2.7MB] completed by the Contract Manager employed by Defence (the signature must match the contract).
- Documentation that evidences:
  - Security policies and plans
  - Annual security awareness program for all staff
  - Insider threat awareness for all staff
  - Employment practices meeting the minimum requirements of Australian Standard 4811-2022
  - Mechanism for the governing body, through the CSO, to approve the annual security reports
  - Policies and procedures which demonstrate the entity which will conduct regular security risk assessments which will be made available to Defence upon request
  - Designated Security Assessed Position (DSAP) list
  - Security register, including overseas travel, incidents, training, other documented controls
  - ICT accreditation (depending on answers to Cyber questionnaire)
  - Facility accreditation, if applying for physical security membership of level 1, 2 or 3

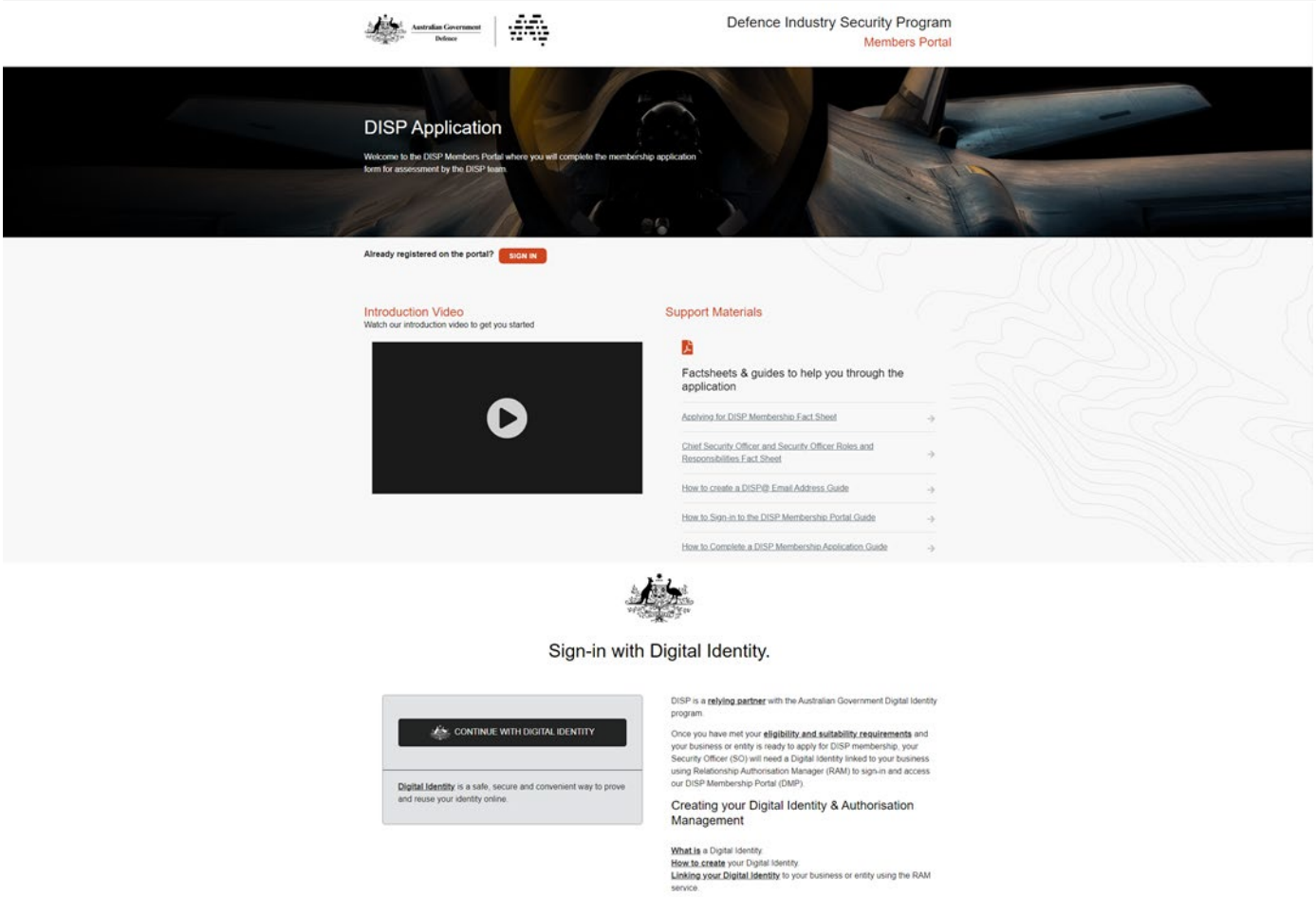
Note: DISP will support you in identifying and creating these documents after submission of your application if required.

Complete the application in the DISP Members Portal

As a DISP Members Portal early release participant, you will be emailed a direct link to the DISP Members Portal to complete your application. You will need to select "Continue with Digital Identity" to sign-in. Support resources will be emailed and available from within the DISP Members Portal.

For more information, refer to the How to Sign-In to the DISP Members Portal Guide.

Note: Only one person can have access to complete the application and it must be an SO but please liaise with your CSO and appropriate staff members to assist with completion.



Filling out the application

The first thing you will need to do when entering the DISP Members Portal will be to update your personal profile. This includes providing your AGSVA Personal Security Clearance details and acknowledging whether you have completed Security Officer Training.

After your profile is complete, there are nine sections of the application that will need to be filled out:

- Entity Details
- Officer Details
- Contracts & Panels
- Physical & ICT
- Membership Levels
- Foreign Ownership, Control & Influence
- Cyber Questionnaire
- Attachments
- Preview & Submit

For Early Release Participants: *Please note that the website still refers to the previous process, but you should apply through the DISP Members Portal and are not required to fill out the AE250 or AE250-1 PDF forms.*

For more information, refer to the How to Complete a DISP Membership Application Guide.

For detailed information, refer to the How to Apply section of the DISP website.

Submit your application and understand what is next

Once your application is complete and **prior to selecting Submit**, please ensure that your CSO has reviewed the application in full, you have updated any required information appropriately and you have double checked the information to ensure its accuracy.

Note: after you select Submit, the SO and the CSO will no longer be able to edit the application.

Your CSO will need to sign-in and complete the declaration in the DISP Members Portal and then your SO can sign-in and submit the application.

The DISP team will then triage your application, prioritising based on factors such as whether you hold or are tendering or negotiating for a Defence contract or panel, or are involved in the shipbuilding supply chain. A DISP processing officer will then contact you to let you know your application is being considered. This person will be your key contact for the DISP membership application from this point forward.

Assuming your entity has all the required clearances, certifications and accreditations and depending on the complexity of the application, processing of the application is expected to take 2–3 months for entry level, and 4–6 months for levels 1, 2 and 3.

Your DISP processing officer will contact you if they require any further information to continue with your application. They will provide you updates at relevant points and will let you know if your membership has been granted or denied.

For more information, including on what happens after your application is submitted, refer to the How to Apply page on the DISP website.

While your application is being processed

It is recommended that all DISP members subscribe to the Australian Security Intelligence Organisation's (ASIO's) Outreach program and the Australian Cyber Security Centre's (ACSC's) Partnership program.

If another entity contacts you with questions about applying for DISP membership and you are not clear on how to answer, please ask them to contact DISP.PortalProject@defence.gov.au.

Information on supporting supply chain entities to apply for DISP membership will be provided to DISP members in the future as part of the DISP Members Portal implementation.

For information on maintaining your DISP membership, refer to the Maintaining Membership page on the DISP website. For information on what ongoing assurance activities are conducted once DISP membership is granted, please visit the Assurance page on the DISP website.

If you require support, please contact DISP.info@defence.gov.au

Australian Government
Defence

DISP

Applying for DISP Membership

FAMILIARISE yourself with the program, framework and requirements

DETERMINE the level of membership you need

ASSESS your ability to meet the requirements and gather documents

COMPLETE the application in the DISP Members Portal

SUBMIT your application and understand what is next

For detailed information, refer to the How to Apply section of the DISP website.

Familiarise yourself with the program, framework and requirements

DISP supports industry to improve their security when engaging with Defence. It is a membership-based program that is a control from the Defence Security Principles Framework (DSPF) [PDF 10,220KB] in assuring that the Government's significant investment in Defence capability is appropriately protected.

The DSPF [PDF 10,220KB] is a principles-based framework intended to support a progressive protective security culture that understands and manages risk, leading to robust security outcomes. Principle 16 and Control 16.1, starting on page 145 of the DSPF [PDF 10,220KB] provide principles, controls and instructions to support Defence industry to understand and manage security risks.

DISP membership enables entities to improve their security operating environment, access Defence security services, training and materials, sponsor their own security clearances, broaden the range of contracts they can tender for and gain advice and analysis on the latest security trends and threats.

Note: your entity only needs one DISP membership regardless of the number of Defence contracts it holds.

To apply for DISP membership, your entity must:

- Be registered in Australia with an ABN.

  For more information, refer to business.gov.au.
- Be financially solvent.
- Have a Chief Security Officer (CSO) and a Security Officer (SO) who meet the requirements set out in the CSO and SO Roles and Responsibilities Fact Sheet and are able to obtain a Digital Identity, such as myGovID, which is linked to your entity via Relationship Authorisation Manager (RAM).

  For support with Digital Identity, please visit www.digitalidentity.gov.au/support.
- Have an established email address in the format of DISP@YourEntityName which is hosted in Australia.

  For more information, refer to the How to Create a DISP@ Email Address Guide.
- Satisfy Defence requirements for Foreign Ownership, Control or Influence (FOCI) [PDF 645KB].
- Not have any relationships with a listed terrorist organisation, regimes subject to United Nations Security Council (UNSC) and Australian autonomous sanctions laws or persons and/or entities on the Department of Foreign Affairs and Trade's (DFAT's) Consolidated List.
- Have an ICT network that meets one of the following cyber security accreditation standards:
  - Top 4 of the Australian Signals Directorate (ASD) Essential 8
  - International Organization for Standardization (ISO/IEC) 27001 and 27002
  - U.S. National Institute of Standards and Technology (NIST) SP 800-171
  - UK Defence Standard (Def Stan) 05-138

Please ensure that you have read and understand the Eligibility and Suitability criteria on the DISP website and Principle 16 and Control 16.1 of the DSPF, starting on page 145 of the DSPF [PDF 10,220KB] prior to applying.

If you require support or have questions, please contact DISP.info@Defence.gov.au.

Australian Government
Defence

DISP

Determine the level of membership you need

There are four DISP Membership levels that align with Australian Government security classifications and four security domains. A membership level for each of the security domains must be selected based on your entity's requirements.

Security Domains:	Personnel Security	Physical Security	Information & Cyber Security	Governance
Questions to answer for membership level selection[1]:	Does your entity require the ability to sponsor and manage security clearances?	*Do you need to handle or store classified (PROTECTED or above) information physically on your company's premises?*[2]	*Do you need to handle or store classified (PROTECTED or above) information or assets on your company's ICT networks?*[2]	*What is the highest level you have selected across the other three domains?*
Entry Level	No, required security clearances will be sponsored by Defence or another government agency	No, my entity only handles or stores OFFICIAL / OFFICIAL: Sensitive information or assets	No, my entity ICT networks only handle or store OFFICIAL / OFFICIAL: Sensitive information	Entry Level (OFFICIAL / OFFICAL: Sensitive)
Level 1[1]	Yes, at the BASELINE (PROTECTED) level[3]	Yes, my entity requires at least one facility/room to be able to handle or store PROTECTED information or assets	Yes, my entity ICT networks require accreditation to handle or store SECRET information[2]	Level 1 (PROTECTED)
Level 2[1]	Yes, up to and including NV1 (SECRET) level[3]	Yes, my entity requires at least one facility/room to be able to handle or store SECRET information or assets	Yes, my entity ICT networks require accreditation to handle or store SECRET information[2]	Level 2 (SECRET)
Level 3[1]	Yes, up to and including NV2 (TOP SECRET) level[3,4]	Yes, my entity requires at least one facility/room to be able to handle or store TOP SECRET information or assets	Yes, my entity ICT networks require accreditation to handle or store TOP SECRET information[2]	Level 3 (TOP SECRET)

[1] Appropriate business case justification must be provided when applying for level 1, 2 or 3 membership; holding a Defence contract alone is not sufficient justification. A higher membership level requires more rigorous, complex and time-consuming application and assessment processes as well as greater governance and administration for the entity including higher costs for physical and ICT infrastructure and accreditation.

[2] Please select Entry Level membership for the Physical Security and Information and Cyber Security domain, unless you have existing certification and accreditation from Defence or an explicit requirement for a higher level to fulfil a current Defence contract.

[3] A DISP Security Officer must have a minimum NV1 clearance to sponsor clearances.

[4] DISP members cannot sponsor Positive Vetting (PV) security clearances; Defence SES Band 3 sponsorship is required to obtain a PV security clearance.

Note: Your membership level may be upgraded or downgraded as appropriate after it is initially granted.

For more information, including examples of entities and the levels for which they should apply, refer to the How to Apply section of the DISP website.

Australian Government
Defence

DISP

Assess your ability to meet the requirements and gather documents

The DISP Membership Requirements Checklist [PDF 188KB] is a key resource to help you answer the required questions prior to applying for DISP membership.

Please ensure that all information you provide about your entity matches the information recorded in the ASIC register, especially your registered business address and ABN/ACN.

Please ensure that you have gathered the following mandatory documentation to support your application:

- Applicant's Security Clearance level and status with CSID (your unique AGSVA ID found on myClearance or clearance emails from AGSVA) and date received, if applicable and Security Officer Training status with completion date and certificate, if applicable.

Note: you are able to proceed with your DISP membership application if you do not yet have a Security Clearance or have not yet completed Security Officer Training. However, membership will not be granted until your SO and CSO receive their clearances and attest to their intent to complete the training.

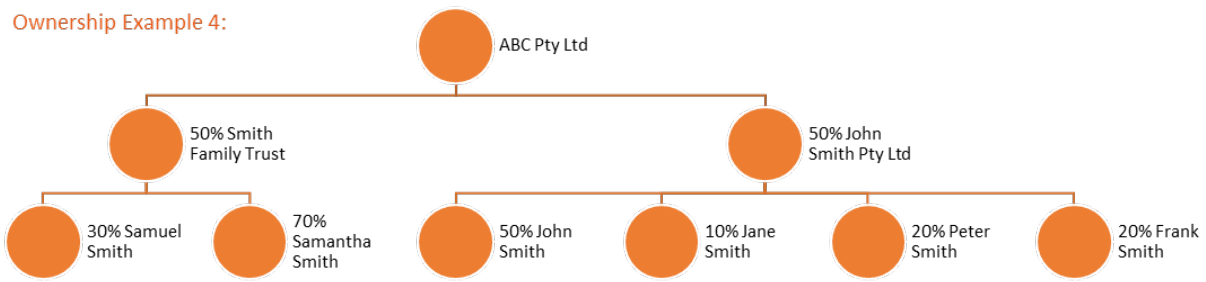
- A statement/list/chart/diagram that depicts the financial ownership of your entity, including all parent companies and their affiliates, ultimate beneficiaries, joint ventures, limited partnerships and subsidiaries.

Ownership Example 1: ABC Pty Ltd is solely owned by John Smith

Ownership Example 2: ABC Pty Ltd shareholding is 100% John Smith

Ownership Example 3: ABC Pty Ltd shareholding is 50% John Smith and 50% Jane Smith

Ownership Example 4:



Further documentation:

Further documentation, such as the following, may be required depending on the level of membership you are applying for and your answers to questions in the application:

- If you have a Defence contract which requires DISP membership, an AE250-2 form [PDF 2.7MB] completed by the Contract Manager employed by Defence (the signature must match the contract).
- Documentation that evidences:
  - Security policies and plans
  - Annual security awareness program for all staff
  - Insider threat awareness for all staff
  - Employment practices meeting the minimum requirements of Australian Standard 4811-2022
  - Mechanism for the governing body, through the CSO, to approve the annual security reports
  - Policies and procedures which demonstrate the entity which will conduct regular security risk assessments which will be made available to Defence upon request
  - Designated Security Assessed Position (DSAP) list
  - Security register, including overseas travel, incidents, training, other documented controls
  - ICT accreditation (depending on answers to Cyber questionnaire)
  - Facility accreditation, if applying for physical security membership of level 1, 2 or 3

Note: DISP will support you in identifying and creating these documents after submission of your application if required.

Australian Government
Defence

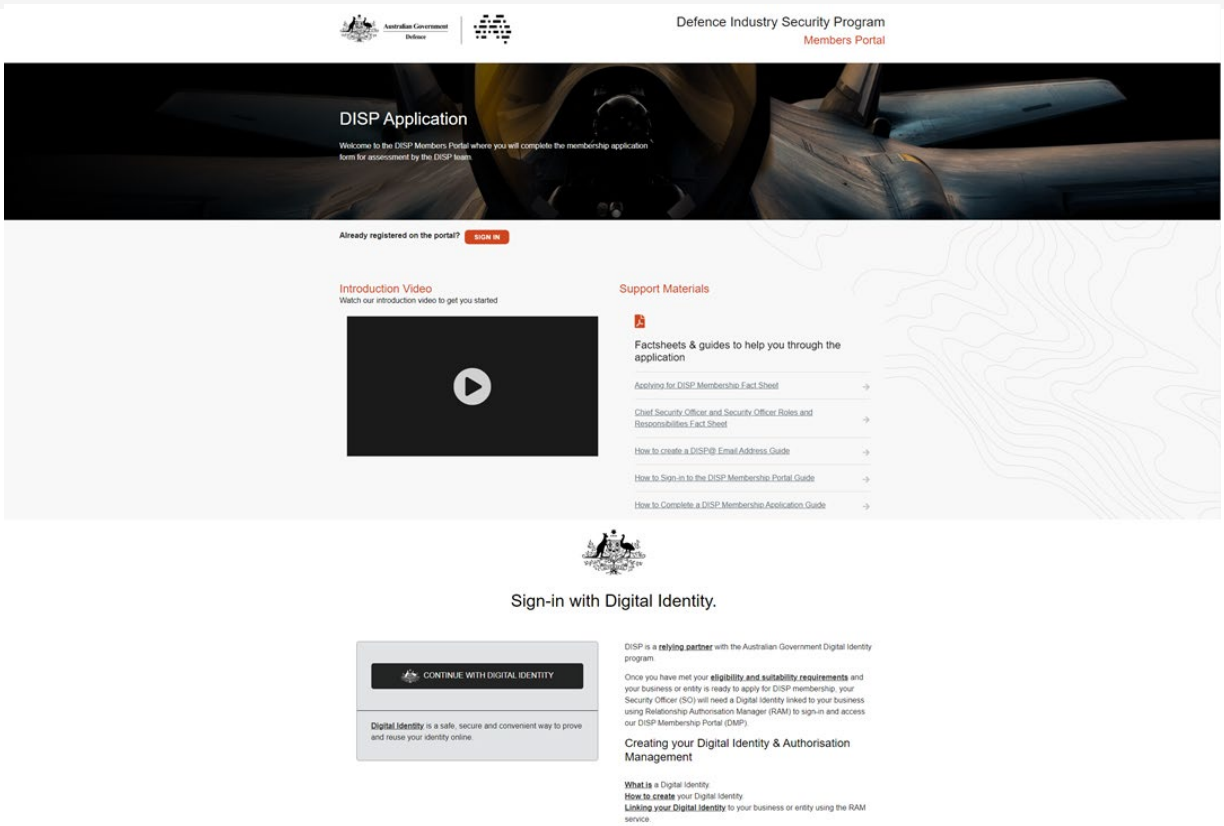
DISP

Complete the application in the DISP Members Portal

As a DISP Members Portal early release participant, you will be emailed a direct link to the DISP Members Portal to complete your application. You will need to select "Continue with Digital Identity" to sign-in. Support resources will be emailed and available from within the DISP Members Portal.

For more information, refer to the How to Sign-In to the DISP Members Portal Guide.

Note: Only one person can have access to complete the application and it must be an SO but please liaise with your CSO and appropriate staff members to assist with completion.



Filling out the application

The first thing you will need to do when entering the DISP Members Portal will be to update your personal profile. This includes providing your AGSVA Personal Security Clearance details and acknowledging whether you have completed Security Officer Training.

After your profile is complete, there are nine sections of the application that will need to be filled out:

- Entity Details
- Officer Details
- Contracts & Panels
- Physical & ICT
- Membership Levels
- Foreign Ownership, Control & Influence
- Cyber Questionnaire
- Attachments
- Preview & Submit

For Early Release Participants: *Please note that the website still refers to the previous process, but you should apply through the DISP Members Portal and are not required to fill out the AE250 or AE250-1 PDF forms.*

For more information, refer to the How to Complete a DISP Membership Application Guide.

For detailed information, refer to the How to Apply section of the DISP website.

Australian Government
Defence

DISP

Submit your application and understand what is next

Once your application is complete and **prior to selecting Submit**, please ensure that your CSO has reviewed the application in full, you have updated any required information appropriately and you have double checked the information to ensure its accuracy.

Note: after you select Submit, the SO and the CSO will no longer be able to edit the application.

Your CSO will need to sign-in and complete the declaration in the DISP Members Portal and then your SO can sign-in and submit the application.

The DISP team will then triage your application, prioritising based on factors such as whether you hold or are tendering or negotiating for a Defence contract or panel, or are involved in the shipbuilding supply chain. A DISP processing officer will then contact you to let you know your application is being considered. This person will be your key contact for the DISP membership application from this point forward.

Assuming your entity has all the required clearances, certifications and accreditations and depending on the complexity of the application, processing of the application is expected to take 2–3 months for entry level, and 4–6 months for levels 1, 2 and 3.

Your DISP processing officer will contact you if they require any further information to continue with your application. They will provide you updates at relevant points and will let you know if your membership has been granted or denied.

For more information, including on what happens after your application is submitted, refer to the How to Apply page on the DISP website.

While your application is being processed

It is recommended that all DISP members subscribe to the Australian Security Intelligence Organisation's (ASIO's) Outreach program and the Australian Cyber Security Centre's (ACSC's) Partnership program.

If another entity contacts you with questions about applying for DISP membership and you are not clear on how to answer, please ask them to contact DISP.PortalProject@defence.gov.au.

Information on supporting supply chain entities to apply for DISP membership will be provided to DISP members in the future as part of the DISP Members Portal implementation.

For information on maintaining your DISP membership, refer to the Maintaining Membership page on the DISP website. For information on what ongoing assurance activities are conducted once DISP membership is granted, please visit the Assurance page on the DISP website.

If you require support, please contact DISP.info@defence.gov.au.