Australian Government

Defence

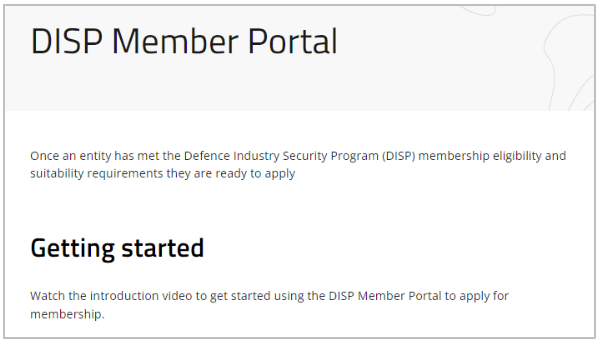
DISP

Cyber Security Questionnaire through the Annual Security Report

I am responsible for:	I need to be able to:
Advising DISB of our Annual Security Report	Access and navigate the Member Portal and complete the Annual Security Report

Step One

Navigate to the DISP Member Portal Page. DISP Member Portal | Business & Industry | Defence



DISP Member Portal

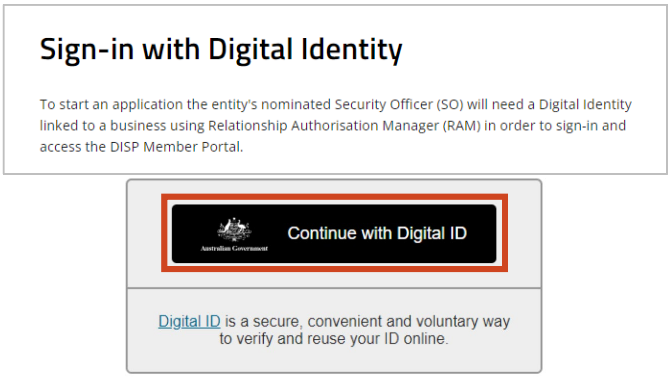
Once an entity has met the Defence Industry Security Program (DISP) membership eligibility and suitability requirements they are ready to apply

Getting started

Watch the introduction video to get started using the DISP Member Portal to apply for membership.

Step Two

Scroll to and *click* '**Continue with Digital Identity**'.



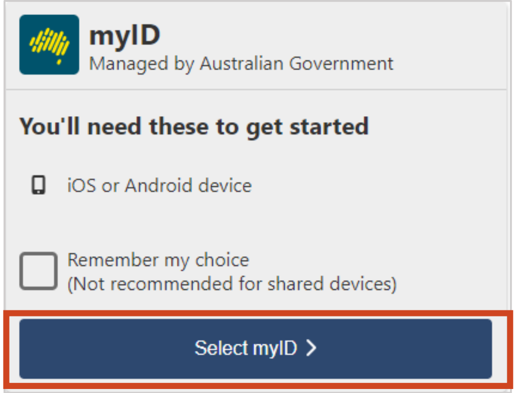
Sign-in with Digital Identity

To start an application the entity's nominated Security Officer (SO) will need a Digital Identity linked to a business using Relationship Authorisation Manager (RAM) in order to sign-in and access the DISP Member Portal.

Digital ID is a secure, convenient and voluntary way to verify and reuse your ID online.

Step Three

Click '**Select MyID**' and *follow* prompts to sign in to access DISP Member Portal.



myID

Managed by Australian Government

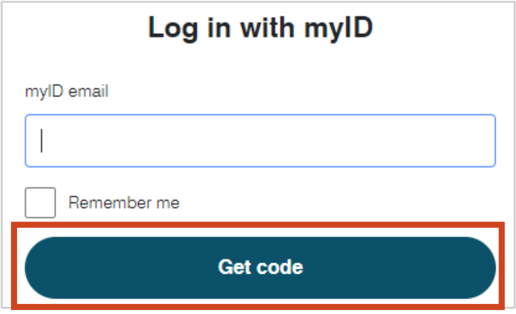
You'll need these to get started

iOS or Android device

□ Remember my choice (Not recommended for shared devices)

Step Four

Enter myID email and *click* '**Get code**'. Enter code into myID app when prompted.



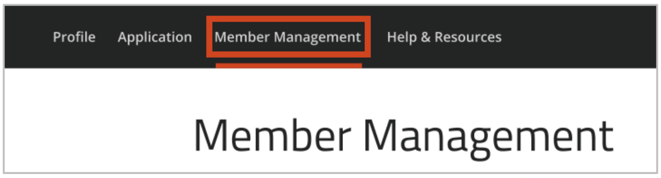
Log in with myID

myID email

□ Remember me

Step Five

Navigate to the banner and *click* '**Member Management**.

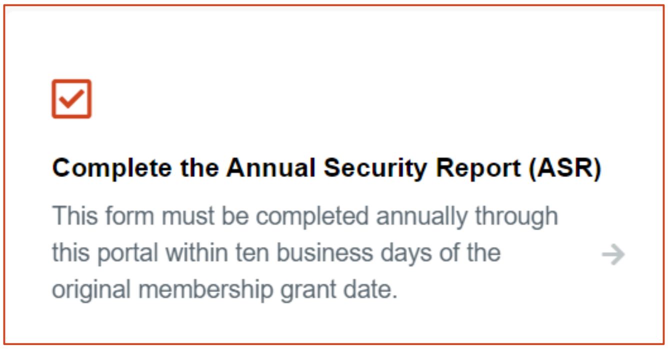


Member Management

Cyber Security Questionnaire through the Annual Security Report

Step Six

Click the ‘**Complete the Annual Security Report (ASR)’** panel.



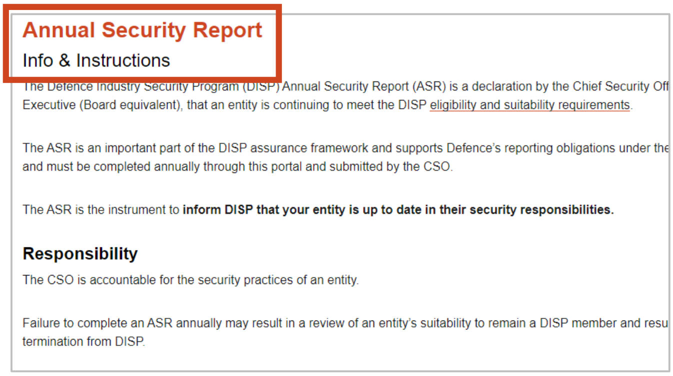
☑

Complete the Annual Security Report (ASR)

This form must be completed annually through this portal within ten business days of the original membership grant date. →

Step Seven

Read the ‘**Info & Instructions**’ page.



Annual Security Report

Info & Instructions

The Defence Industry Security Program (DISP) Annual Security Report (ASR) is a declaration by the Chief Security Off Executive (Board equivalent), that an entity is continuing to meet the DISP eligibility and suitability requirements.

The ASR is an important part of the DISP assurance framework and supports Defence's reporting obligations under the and must be completed annually through this portal and submitted by the CSO.

The ASR is the instrument to **inform DISP that your entity is up to date in their security responsibilities.**

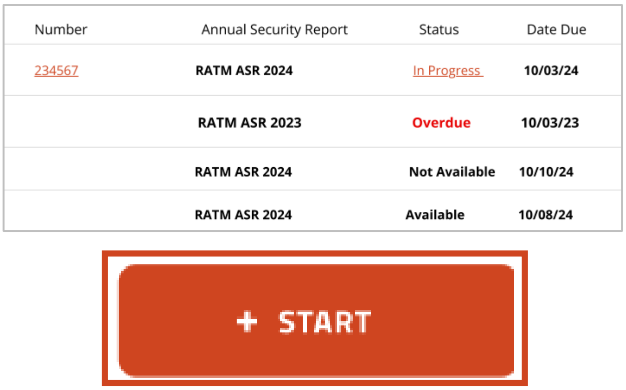
Responsibility

The CSO is accountable for the security practices of an entity.

Failure to complete an ASR annually may result in a review of an entity's suitability to remain a DISP member and resu termination from DISP.

Step Eight

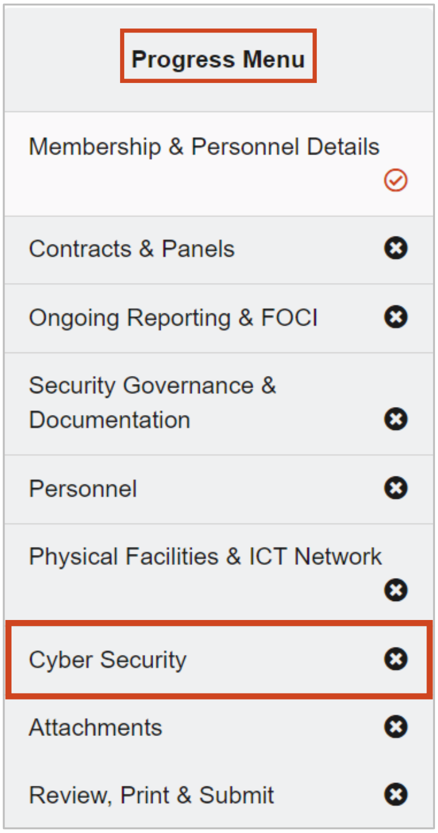
Click **‘Start’** to begin the Annual Security Report Application.



Number	Annual Security Report	Status	Date Due
234567	**RATM ASR 2024**	In Progress	**10/03/24**
	RATM ASR 2023	**Overdue**	**10/03/23**
	RATM ASR 2024	**Not Available**	**10/10/24**
	RATM ASR 2024	**Available**	**10/08/24**

Step Nine

Populate the fields as instructed on each page of the ‘**Progress Menu**’ up to ‘**Cyber Security**’.

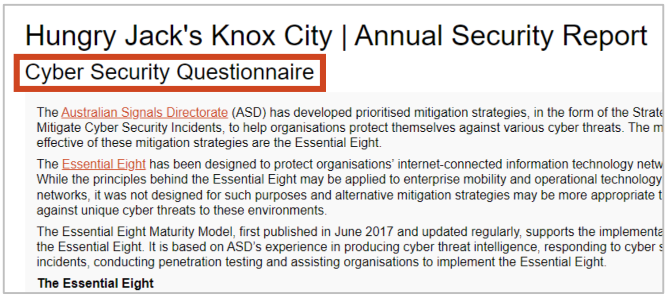


Progress Menu

- Membership & Personnel Details ✓
- Contracts & Panels ☒
- Ongoing Reporting & FOCI ☒
- Security Governance & Documentation ☒
- Personnel ☒
- Physical Facilities & ICT Network ☒
- Cyber Security ☒
- Attachments ☒
- Review, Print & Submit ☒

Step Ten

Read the ‘**Cyber Security Questionnaire’** page.



Hungry Jack's Knox City | Annual Security Report

Cyber Security Questionnaire

The Australian Signals Directorate (ASD) has developed prioritised mitigation strategies, in the form of the Strate Mitigate Cyber Security Incidents, to help organisations protect themselves against various cyber threats. The m effective of these mitigation strategies are the Essential Eight.

The Essential Eight has been designed to protect organisations' internet-connected information technology netw While the principles behind the Essential Eight may be applied to enterprise mobility and operational technology networks, it was not designed for such purposes and alternative mitigation strategies may be more appropriate t against unique cyber threats to these environments.

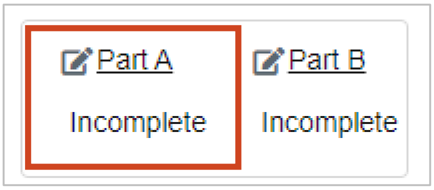
The Essential Eight Maturity Model, first published in June 2017 and updated regularly, supports the implementa the Essential Eight. It is based on ASD's experience in producing cyber threat intelligence, responding to cyber s incidents, conducting penetration testing and assisting organisations to implement the Essential Eight.

The Essential Eight

Cyber Security Questionnaire through the Annual Security Report

Step Eleven

Click '**Part A**' at the bottom of the page.

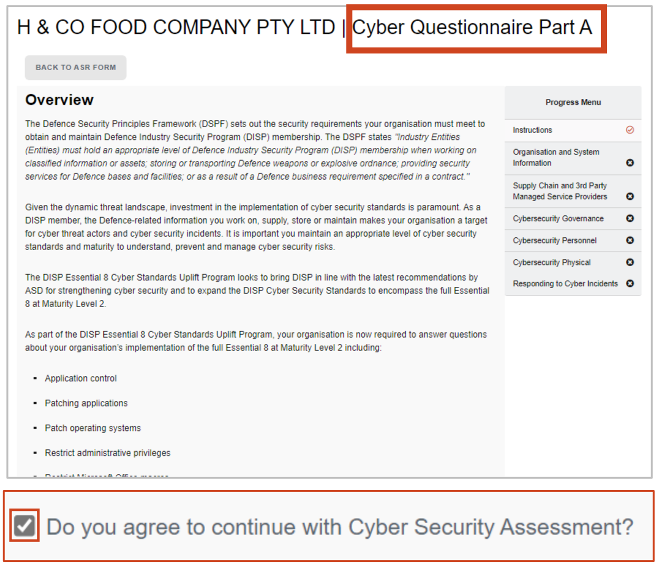


Part A
Incomplete

Part B
Incomplete

Step Twelve

Read the '**Cyber Security Questionnaire Part A**' page, then *click* on the tick box at the bottom.



H & CO FOOD COMPANY PTY LTD | Cyber Questionnaire Part A

Overview

The Defence Security Principles Framework (DSPF) sets out the security requirements your organisation must meet to obtain and maintain Defence Industry Security Program (DISP) membership. The DSPF states *"Industry Entities (Entities) must hold an appropriate level of Defence Industry Security Program (DISP) membership when working on classified information or assets; storing or transporting Defence weapons or explosive ordnance; providing security services for Defence bases and facilities; or as a result of a Defence business requirement specified in a contract."*

Given the dynamic threat landscape, investment in the implementation of cyber security standards is paramount. As a DISP member, the Defence-related information you work on, supply, store or maintain makes your organisation a target for cyber threat actors and cyber security incidents. It is important you maintain an appropriate level of cyber security standards and maturity to understand, prevent and manage cyber security risks.

The DISP Essential 8 Cyber Standards Uplift Program looks to bring DISP in line with the latest recommendations by ASD for strengthening cyber security and to expand the DISP Cyber Security Standards to encompass the full Essential 8 at Maturity Level 2.

As part of the DISP Essential 8 Cyber Standards Uplift Program, your organisation is now required to answer questions about your organisation's implementation of the full Essential 8 at Maturity Level 2 including:

- Application control
- Patching applications
- Patch operating systems
- Restrict administrative privileges

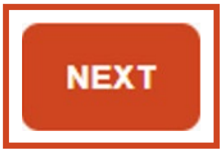
Progress Menu

Instructions ✓
Organisation and System Information ☒
Supply Chain and 3rd Party Managed Service Providers ☒
Cybersecurity Governance ☒
Cybersecurity Personnel ☒
Cybersecurity Physical ☒
Responding to Cyber Incidents ☒

☑ Do you agree to continue with Cyber Security Assessment?

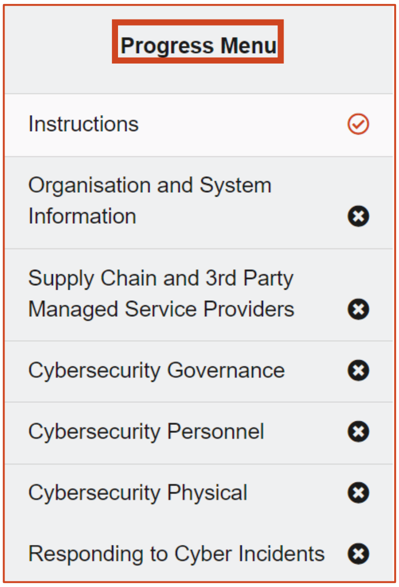
Step Thirteen

Click '**Next**'.



Step Fourteen

Populate the fields as instructed on each page of the '**Progress Menu**'.

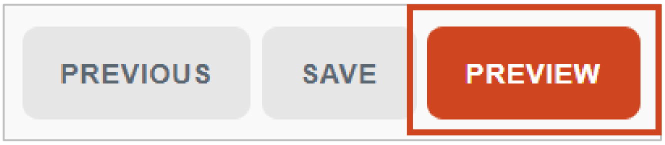


Progress Menu

Instructions ✓
Organisation and System Information ☒
Supply Chain and 3rd Party Managed Service Providers ☒
Cybersecurity Governance ☒
Cybersecurity Personnel ☒
Cybersecurity Physical ☒
Responding to Cyber Incidents ☒

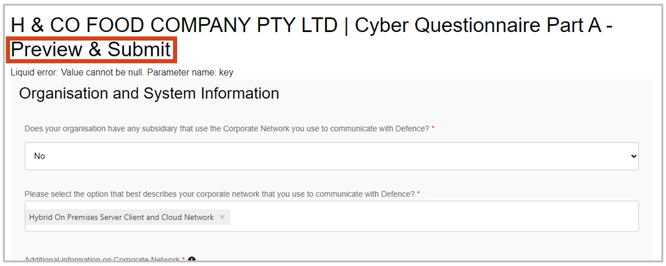
Step Fifteen

Click '**Preview**'.



Step Sixteen

Finalise the fields as instructed on '**Preview & Submit**' page.



H & CO FOOD COMPANY PTY LTD | Cyber Questionnaire Part A - Preview & Submit

Liquid error: Value cannot be null. Parameter name: key

Organisation and System Information

Does your organisation have any subsidiary that use the Corporate Network you use to communicate with Defence? *

No

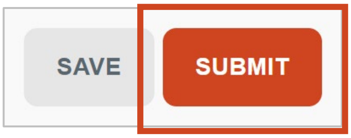
Please select the option that best describes your corporate network that you use to communicate with Defence? *

Hybrid On Premises Server Client and Cloud Network ×

Cyber Security Questionnaire through the Annual Security Report

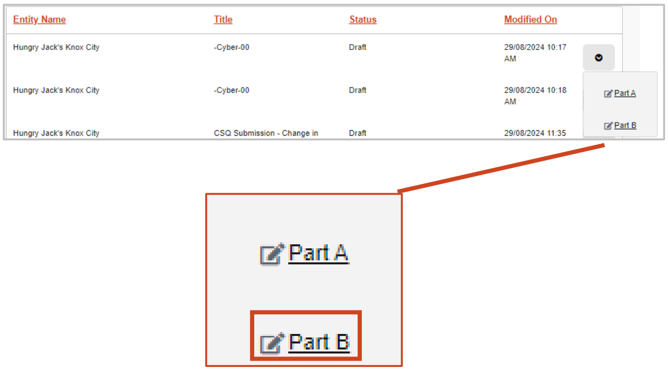
Step Seventeen

Click ‘**Submit**’.



Step Eighteen

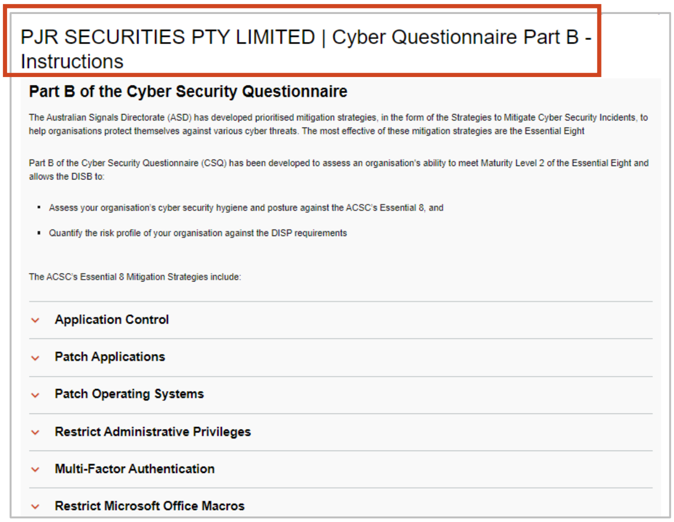
Click ‘**Part B**’.



Entity Name	Title	Status	Modified On
Hungry Jack's Knox City	-Cyber-00	Draft	29/08/2024 10:17 AM
Hungry Jack's Knox City	-Cyber-00	Draft	29/08/2024 10:18 AM
Hungry Jack's Knox City	CSQ Submission - Change in	Draft	29/08/2024 11:35

Step Nineteen

Read the ‘**Cyber Security Questionnaire Part B-Instructions**’ page, then *click* ‘**Next**’.



PJR SECURITIES PTY LIMITED | Cyber Questionnaire Part B - Instructions

Part B of the Cyber Security Questionnaire

The Australian Signals Directorate (ASD) has developed prioritised mitigation strategies, in the form of the Strategies to Mitigate Cyber Security Incidents, to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight

Part B of the Cyber Security Questionnaire (CSQ) has been developed to assess an organisation's ability to meet Maturity Level 2 of the Essential Eight and allows the DISB to:

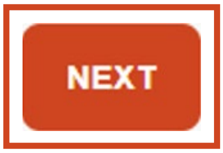
- Assess your organisation's cyber security hygiene and posture against the ACSC's Essential 8, and
- Quantify the risk profile of your organisation against the DISP requirements

The ACSC's Essential 8 Mitigation Strategies include:

- Application Control
- Patch Applications
- Patch Operating Systems
- Restrict Administrative Privileges
- Multi-Factor Authentication
- Restrict Microsoft Office Macros

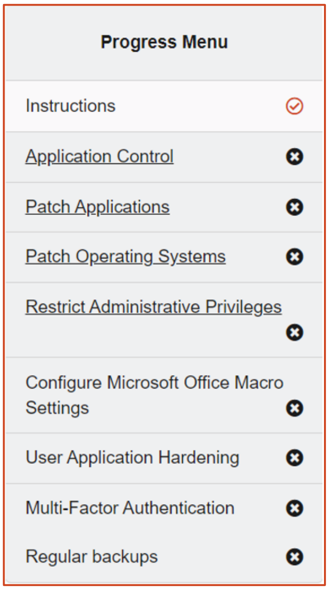
Step Twenty

Click ‘**Next**’.



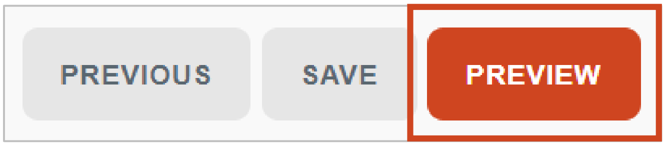
Step Twenty-one

Populate the fields as instructed on each page of the ‘**Cyber Security Questionnaire Part B’** menu.


Progress Menu
Instructions
Application Control
Patch Applications
Patch Operating Systems
Restrict Administrative Privileges
Configure Microsoft Office Macro Settings
User Application Hardening
Multi-Factor Authentication
Regular backups

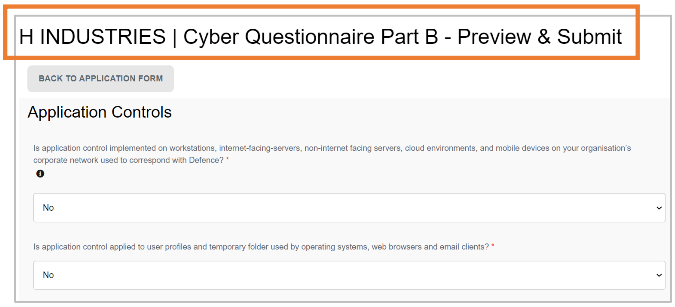
Step Twenty-two

Click ‘**Preview’**.



Step Twenty-three

Finalise the fields as instructed on ‘**Preview & Submit**‘ page.



H INDUSTRIES | Cyber Questionnaire Part B - Preview & Submit

Application Controls

Is application control implemented on workstations, internet-facing-servers, non-internet facing servers, cloud environments, and mobile devices on your organisation’s corporate network used to correspond with Defence? *

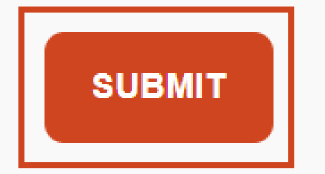
No

Is application control applied to user profiles and temporary folder used by operating systems, web browsers and email clients? *

No

Step Twenty-four

Click ‘**SUBMIT**’.



Help and Support

For further support please email
DISP.info@defence.gov.au

Please don’t hesitate to share your feedback on these instructions upon completion of testing.

NOTE: Information available is subject to change as the DMS matures.