Australian Government
Attorney-General's Department

Protective Security Policy Framework

PSPF reporting portal—quick start guide

The PSPF reporting portal allows Commonwealth entities to complete and submit their annual security maturity self-assessment online, access benchmarking reports at the conclusion of the submission period and, from 2019-20, access assessments and reports from previous reporting periods.

Before accessing the portal, users should be familiar with the Protective Security Policy Framework (PSPF)—the full PSPF is available at www.protectivesecurity.gov.au. The portal has been designed to support entities to meet their reporting obligations under PSPF Policy 5: Reporting on security.

Accessing the portal

Registered users can access the portal through the link located under the home tab on the PSPF website www.protectivesecurity.gov.au.

Account activation

New users will receive an email with a link to activate your account on the portal. Follow the link and complete the online registration.

You will be asked to accept the conditions for access and to create a password that meets the complexity requirements set out in the Australian Government Information Security Manual.

The link in your activation email will expire after 48 hours. If you need a new activation link contact your Chief Security Officer (CSO) or entity user administrator.

Note! The Attorney-General's Department maintains a list of all CSOs. CSOs accessing the portal for the first time will automatically receive their account activation email at the start of the assessment period.

To request changes to an entity's CSO details, contact the PSPF reporting team at PSPFreporting@ag.gov.au or on 02 6141 3600.

Logging in

Logging in to the portal uses two-factor authentication.

- **Factor 1—Username and password**
  - Your username is your registered email address. If you forget your password, click on the 'Forgot Password?' link.
- **Factor 2—One-time passcode**
  - When you enter your username and password, the portal will send you an email with a one-time passcode. You will need to enter the one-time passcode within 3 minutes.

Requesting access

The entity's CSO or their delegated entity user administrator manages access to the portal. Contact your CSO or user administrator to request access to the portal or changes to your user role, or if you need a new activation link.

Note! If user changes are required and the CSO and entity user administrator are not available, contact the PSPF reporting team at PSPFreporting@ag.gov.au or on 02 6141 3600.

The assessment process

There are four processes to complete and submit the annual security maturity self-assessment online.

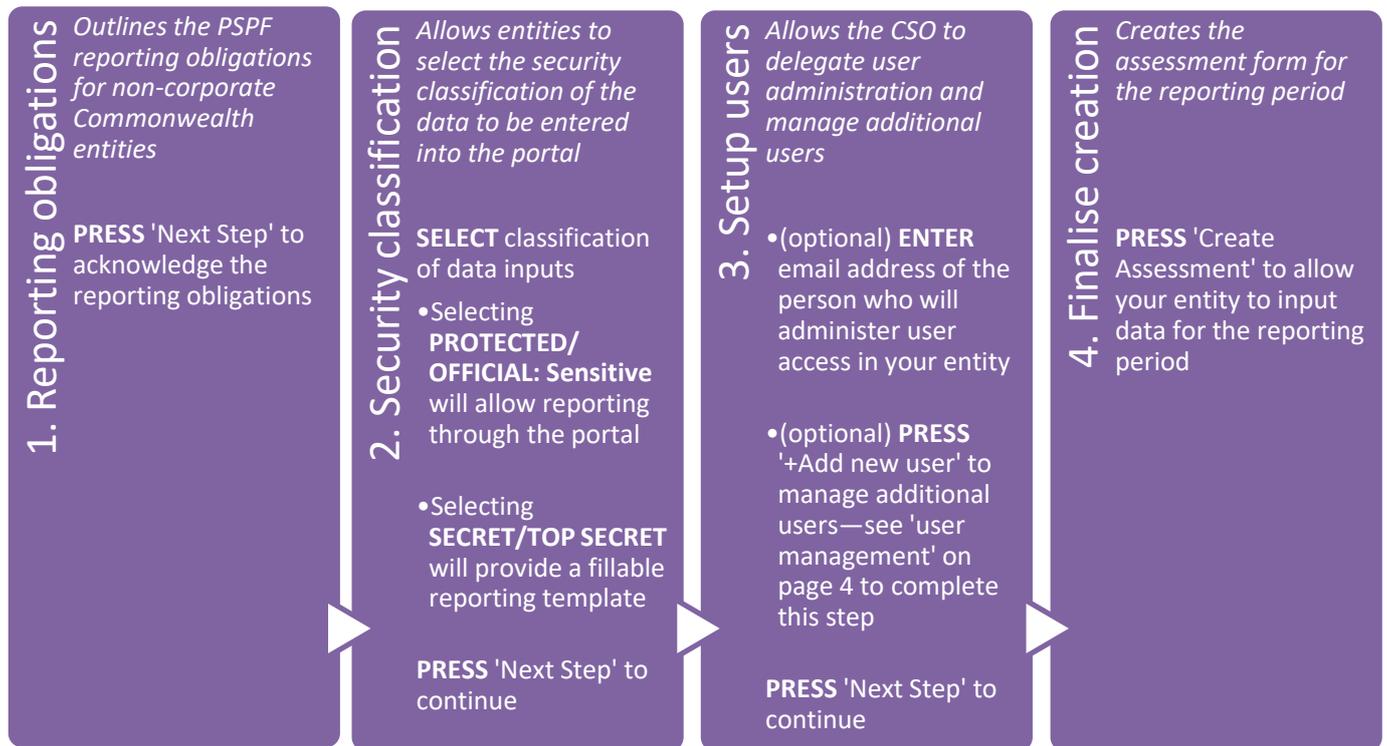**Figure 1 PSPF assessment flow chart**
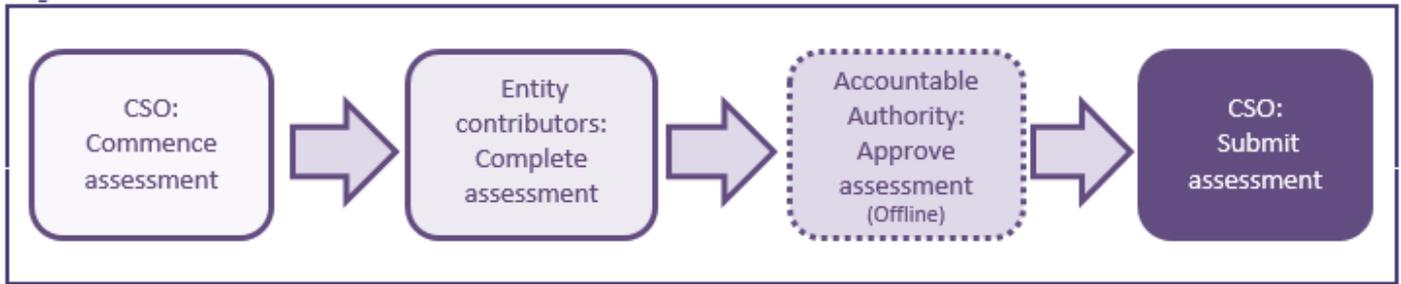
The portal requires the CSO to complete two of the four processes:

- the CSO must commence the assessment
- the CSO must submit the assessment

The CSO can assign responsibility for completing the assessment to other users. The Accountable Authority must approve the final assessment offline. The portal will generate a printable assessment (in Microsoft Word) which can be approved by the Accountable Authority through standard entity procedures.

Commencing the assessment—must be done by the CSO

At the start of the new assessment period, all CSOs will receive an email advising that the PSPF assessment for the entity is available for completion. The email will provide a link to login and indicate the due date for submission. The CSO must complete the following four steps to start the assessment for the entity:

1. Reporting obligations

Outlines the PSPF reporting obligations for non-corporate Commonwealth entities

PRESS 'Next Step' to acknowledge the reporting obligations

2. Security classification

Allows entities to select the security classification of the data to be entered into the portal

SELECT classification of data inputs

- Selecting **PROTECTED/ OFFICIAL: Sensitive** will allow reporting through the portal

- Selecting **SECRET/TOP SECRET** will provide a fillable reporting template

PRESS 'Next Step' to continue

3. Setup users

Allows the CSO to delegate user administration and manage additional users

- (optional) **ENTER** email address of the person who will administer user access in your entity

- (optional) **PRESS** '+Add new user' to manage additional users—see 'user management' on page 4 to complete this step

PRESS 'Next Step' to continue

4. Finalise creation

Creates the assessment form for the reporting period

PRESS 'Create Assessment' to allow your entity to input data for the reporting period

Note! For Chief Security Officers (CSOs) accessing the portal for the first time, please see the account activation information on Page 1.

Completing assessment—can be done by all entity contributors

The annual security maturity self-assessment is comprised of 17 modules—one for each of the 16 PSPF polices and a summary module. Contributors complete the modules to which they have access and modules can have multiple contributors.

The portal displays the most recent data input and will override any previous input. Contributors can use the Notes function (at the bottom of each screen) to indicate to other contributors if they have changed input or want to query previous input. The Notes function is only visible to the entity and does not form part of the assessment submission.

Modules 1-16

The assessment contains a module for each of the 16 PSPF policies. Each of these modules has two parts:

- **Maturity questions**
  - Each module consists of a set of questions drawn from the core and supporting requirements in the PSPF.
- **Rationale, strategies & timeframes**
  - Based on the entity's answers to the maturity questions, the portal will suggest a maturity level for the module. This will be displayed on a chart that shows the distribution of the entities answers for the module.
  - The entity can confirm the suggested maturity level or select a higher or lower maturity level to reflect the entity's self-assessment.
  - There is a text box to enter a rationale for the selected maturity level. If the entity changed the suggested maturity level, the rationale should explain why the change is justified.
  - If the maturity level for the module is ad hoc or developing, there will be a text box to enter the proposed strategies and timeframes to improve the entities maturity level.

After completing a module, the contributor can continue to the incomplete module they have access to or proceed to the summary module to add key risks that are relevant to the module.

Summary Module

The summary module provides the final assessment of the entity's overall maturity level and maturity levels for each of the PSPF outcomes. These are calculated from the entity's self-assessment at each module.

The summary module also includes three text boxes that must be completed:

- **Summary of risk environment and security capability**
- **Key risks to the entity's people, information and assets**
- **Summary of significant security incidents during the reporting period**

The following information will be prefilled from answers provided in earlier modules:

- Exceptional circumstances (if applicable)—prefilled from Module 1 Role of the accountable authority
- Personnel security clearance waivers—prefilled from Module 12 Eligibility and suitability of personnel and Module 13 Ongoing assessment of personnel

Summary module information can be entered by contributors at any time while the assessment is open.

Approving the assessment—must be completed offline

When all modules are complete, the entity's Accountable Authority must approve the final assessment. To generate a printable (Word) version of the assessment press 'Download completed assessment (DOCX)' on the top of any module screen. The printed report provides a place for the Accountable Authority to sign to indicate approval.

Submitting the assessment—must be completed by the CSO

Once the Accountable Authority has approved the assessment report a copy must be sent to the entity's portfolio minister. The CSO can then complete the acknowledgement of reporting obligations and press submit to send the assessment report to the Attorney-General's Department.

User management

The portal has four different user roles to control access and permissions, allowing entities to establish reporting processes that are appropriate to their entity's size, organisation structure and governance arrangements.

Table 1 Roles and responsibilities

Role	Access and permissions	What this means
Submitter	– Commence the annual assessment – Manage entity users – Contribute to all modules – Use Notes function – Provide the final assessment to the accountable authority – Complete the final assessment page – Submit the final assessment through the portal to the Attorney-General's Department	You are the key contact for the assessment and you have been assigned the submitter role. Depending on the size of your entity and your entity's reporting governance arrangements you will manage users' access the portal or assign this function to an entity administrator. Even if you delegate this function, you can continue to manage users. As soon as entity users are assigned roles the users can access the assessment and complete or review their nominated modules. As CSO, you can also contribute to and review the modules. Once the 16 modules have been completed you will finalise the submission information, obtain approval for the assessment from the accountable authority, provide the assessment to the relevant portfolio minister and submit the assessment to the Attorney-General's Department.
Entity Administrator	– Manage entity users	The CSO has delegated the user administration of the portal to you. You will only see information on the users and be able to edit their details, add new users or deactivate existing users. If you are required to see assessment information, the CSO can assign you an entity viewer role.
Contributor	– Contribute to assigned modules and the summary module – Use Notes function	As a contributor you will be assigned modules to complete. Your entity reporting process will determine whether you need to answer some or all maturity questions and what other data you need to input. This may include – determining the self-assessed maturity level for modules you have been assigned – providing a rationale for the maturity level and where you have varied the maturity level from the suggested maturity level – providing strategies and timelines to improve the maturity level if the module has been assessed at ad-hoc or developing – identifying key risks to the entity's people, information and assets. You may also be assigned entity viewer access to other modules. You can see details of all the portal users and can change your own contact details.
Entity Viewer	– View assessment information, reports, users and modules they have been given access to – Use Notes function	As an entity viewer you can access all the portal reports, see all the users and see draft and completed modules to which you have been given access. Any feedback to the CSO or module contributor(s) you wish to provide is actioned outside the reporting portal.

The role of Submitter is assigned by the Attorney-General's Department and can only be undertaken by the entity CSO. Other user roles can be assigned by the CSO, including delegation of user management by assigning the role of Entity Administrator.

Table 2 Example scenarios based on the entity size

Small	Medium	Large
CSO commences assessment	CSO commences assessment	CSO commences assessment
CSO manages users	Separate user administrator	Separate user administrator(s)
CSO and one or two contributors input data for all modules	A number of contributors for each module and outcomes	Lead contributors for some outcomes/modules Several contributors per module
CSO reviews all modules	A number of reviewers	Several reviewers
Viewers are limited	Viewers are limited	Many viewers
CSO obtains accountable authority approval	CSO obtains accountable authority approval	CSO obtains accountable authority approval
CSO submits	CSO submits	CSO submits