Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

RackTop SHIELD v1.0

Version 1.0, 2 November 2026

Document reference: AISEP-CC-CR-2026-EFT-T067-CR-V1.0
(Certification expires five years from certification report date)

Table of contents

Executive Summary 1

Introduction 2

Overview 2

Purpose 2

Identification 2

Target of Evaluation 4

Overview 4

Description of the TOE 4

TOE Functionality 4

TOE Physical Boundary 4

Architecture 5

Clarification of Scope 6

Security Policy 7

Secure Delivery 7

Version Verification 7

Documentation and Guidance 8

Secure Usage 8

Evaluation 10

Overview 10

Evaluation Procedures 10

Functional Testing 10

Penetration Testing 10

Certification 12

Overview 12

Assurance 12

Certification Result 12

Recommendations 12

Annex – References and Abbreviations **14**

References 14

Abbreviations 15

Executive Summary

This report describes the findings of the IT security evaluation of RackTop Systems RackTop SHIELD v1.0 product against Common Criteria approved *Protection Profile (PP).*

This report concludes that the Target of Evaluation (TOE) has complied with the following *PP [4]*:

- collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, 01 February 2019 (CPP_FDE_AA_V2.0E).

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australian Information Security Evaluation Program (AISEP). The evaluation was performed by Teron Labs with the final *Evaluation Technical Report (ETR) [7]* submitted on 09 October 2026.

With regard to the secure operation of the TOE, the Australian Certification Authority recommends The users should make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings.

- Users of the TOE shall ensure that the Baseboard Management Controller (BMC) functionality is disabled following the setup of the TOE, per section 2.2.1 of the *guidance document [6].*
- Users to note that installation of the TOE image is only possible through the BMC, the product environment during the process of installation is not considered a CC compliant environment.
- Users of the TOE shall be aware that losing the PIN files or the USB they are stored on will lead to complete loss of access to data on the TOE.
- Once Self-Encrypting Drives (SEDs) are unlocked, SSH may be used to access the inner layer RHEL OS, however no assurance is provided for this functionality.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the *Security Target [8]* and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the TOE.

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the *Common Criteria [1,2,3]* and *Protection Profile [4]*
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's *Security Target [8]* which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is RackTop SHIELD v1.0.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	RackTop SHIELD v1.0
TOE Type	Full Drive Encryption
Software version	SHIELD v1.0
Security Target	Security Target, RackTop Systems, Inc. RackTop SHIELD v1.0, version 1.2, 06 October 2026
Evaluation Technical Report	Evaluation Technical Report 1.0, dated 09 October 2026 Document reference EFT-T067-ETR 1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, April 2017, Version 3.1 Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5
Conformance	collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, 01 February 2019 (CPP_FDE_AA_V2.0E)

Developer	RackTop Systems 13454 Sunrise Valley Drive Suite 550 , Herndon, VA 20171 United States of America
Evaluation facility	Teron Labs Level 2, 14 Moore St, Canberra ACT 2601 Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

The TOE is RackTop SHIELD v1.0, an authorisation acquisition product that obtains and manages authorisation data used to access encrypted data stored on Trusted Computing Group (TCG)-compliant SEDs utilising FIPS 140-2 or 140-3 validated cryptographic modules.

The TOE provides authorisation acquisition and drive unlock functionality as part of a two-layer encryption strategy in accordance with US NSA's Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package guidance *[13]*, specifically fulfilling the Outer Layer Encryption role. It ensures that storage media remains inaccessible unless proper authorisation data is presented in the form of 256-bit keys protected by physical separation from the host system.

Please visit *https://www.nsa.gov* for more information on CSfC Capability Packages.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.6 of the *Security Target [8].*

TOE Physical Boundary

The physical boundary of the TOE includes all hardware and software parts and the security guidance of the TOE. The parts of the TOE included in the physical boundary are detailed in Table 1 below:

Part of the TOE	Identification	Description
TOE Software	RackTop SHIELD v1.0	TOE software is distributed as an ISO package. The following ISO installation packages are used for the TOE: ▪ rhel-9-CSFC-20260626-d01c26e7.iso
Security Guidance	RackTop Guidance Documentation Supplement Version 0.8	The Common Criteria Guidance supplement for the TOE. The security guidance is distributed as a document in PDF format.

Table 1 – Parts Included in the Physical Scope of the TOE

The TOE was evaluated using the hardware and operational-environment configuration identified below. These components provided the platform on which the TOE was installed and tested. However, they do not form part of the

TOE physical boundary. Inclusion in the tested configuration does not imply that the component are independently evaluated as part of the TOE.

- **Processor:** Intel(R) Xeon(R) D-2796NT CPU @ 2.00GHz
- **Motherboard:** Supermicro X12SDV-20C-SPT8F
- **Operating system:** RHEL v9.4
- **Crypto module:** OpenSSL 3.x with FIPS provider 3.0.7
- **OS Drive:** DIGISTOR 2TB fw: ECPG13.0
- **Data Drive:** XP12800LE70025 fw: SE4SA54T

Architecture

The TOE is comprised exclusively of the eboot UEFI application and it's supporting runtime components. The TOE executes during the early boot phase, prior to the initialisation of the operating system, and is responsible for critical functions related to the secure initialisation and unlocking of Self-Encrypting Drives (SEDs).

The TOE is designed to be deployed as the Outer Encryption Layer in a CSfC-compliant two-layer DAR solutions. The TOE simplifies deployment of SED-based encryption and facilitates secure key handling without reliance on enterprise key management infrastructure.

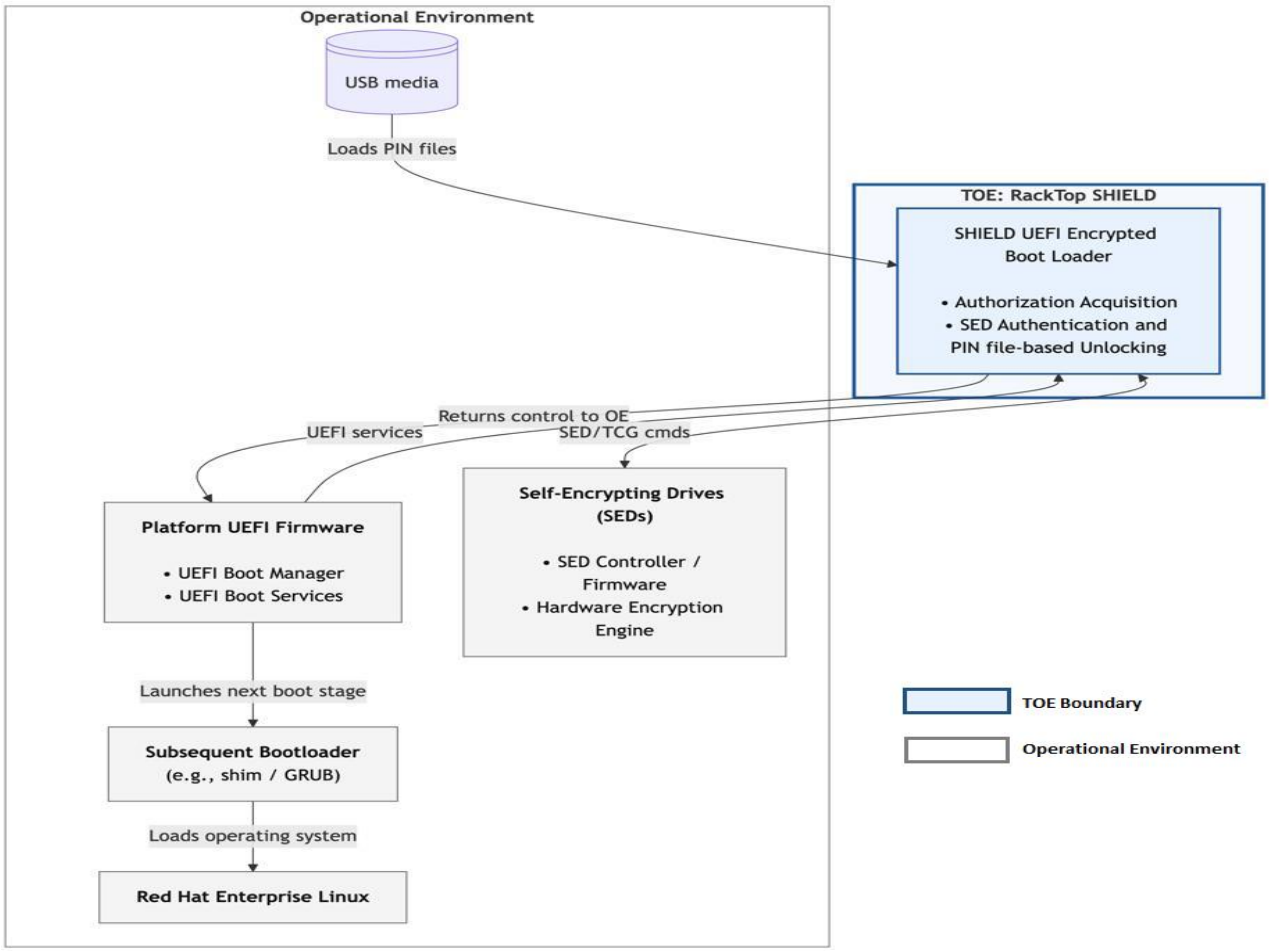


Figure 1 - TOE Architecture

Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the *Security Target [8].*

Evaluated Functionality

Functional tests performed during the evaluation were taken from the *Protection Profile [4]* and *Supporting Document [11]* and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

Non-TOE Hardware/Software/Firmware

The TOE is solely the authorisation acquisition product. Yet, it does require following external components to operate securely and as evaluated. These items are outside the TOE boundary and must be present and correctly configured in the operational environment.

- Operating System

- The TOE does not provide its own entropy source for encryption key generation.
- Self-Encrypting Drives (SEDs)

Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Australian Government and Enterprise users should refer to the *ASD Essentials [14]* for guidance on using the certified product in an enterprise, operational technology or government system. Australian Government users should refer to the *Australian Government Information Security Manual [5]* for policy relating to using an evaluated product in an unevaluated configuration.

Security Policy

The TOE Security Policy is a set of rules that defines the required security behaviour of the TOE; how information within the TOE is managed and protected. The *Security Target [8]* contains a summary of the functionality that is evaluated.

Secure Delivery

The TOE delivery and installation procedures are described in the *Configuration Guidance [6].* The guidance document outlines the required procedures for obtaining and installing the TOE. The TOE software is delivered electronically through the RackTop Systems website.

Installation of the TOE

The *Configuration Guides [6]* contains all relevant information for the secure configuration of the TOE.

Version Verification

Potential user of the TOE can confirm that they have received the product from RackTop Systems by ensuring they downloaded it from *https://www.racktopsystems.com/shield*.

The exact ISO filename should match “rhel-9-CSFC-20260626-d01c26e7.iso” with SHA2-256 hash “5BA29FB776BE50BFE9D94827AFEF53D5264F832D20C30D1EE9F3C98667BE3AF6”.

Additionally, after installation of the product, customers can confirm they have received the correct evaluated version of the product by checking the installed version of the TOE relevant SHIELD RPMs:

- encrypted-boot-1.1.0_rel.55-1.el9.x86_64.rpm
- updatefde-1.0.2-44.el9.noarch.rpm
- shieldadm-1.0.0-10.el9.x86_64.rpm

Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased by the consumer, and it is titled as:

- *RackTop Systems Inc. RackTop SHIELD v1.0 Guidance Supplement, Version 0.8, 21 September 2026*

All Common Criteria guidance material is available at *https://www.commoncriteriaportal.org*.

The *Australian Government Information Security Manual* is available at *https://www.cyber.gov.au/ism [5].*

The *ASD Essentials* are available at *https://www.cyber.gov.au/essentials [14].*

Secure Usage

The evaluation of the TOE took into account certain assumptions concerning its operational environment. These assumptions must remain valid to ensure that the TOE is installed, configured and operated in accordance with its evaluated configuration and that the applicable security objectives are met.

The TOE and its host platform are assumed to be located within a physically secure environment that restricts access to authorised personnel. The physical protection provided by the operational environment is expected to prevent unauthorised access to the TOE, the host platform, connected Self-Encrypting Drives, external USB authorisation media and associated physical interfaces.

The Self-Encrypting Drives used with the TOE are assumed to be placed into service in an appropriate initial state and configured in accordance with the security guidance. Administrators are responsible for ensuring that the drives have not previously contained sensitive information protected by an unknown or superseded encryption key and that the applicable locking ranges, authorisation values and encryption functionality are correctly configured before operational use.

The host platform is assumed to provide appropriate identification and authentication mechanisms independently of the authorisation factor used by the TOE. Administrators must ensure that platform credentials are suitably strong, protected from unauthorised disclosure and managed in accordance with organisational security policies. Any default credentials must be replaced before the TOE is placed into operational service.

The operational environment is assumed to provide the cryptographic functionality and random-bit generation services relied upon by the TOE. These services must be configured and operated in accordance with the evaluated configuration and the applicable security guidance. Administrators must ensure that only the evaluated versions and configurations of the required cryptographic components are used.

External USB media containing the authorisation-factor files must be used only for their intended purpose and securely protected from unauthorised access, modification, duplication or substitution. Administrators must maintain appropriate control over the USB media throughout its lifecycle and securely sanitise or destroy the media when it is no longer required.

The host platform must be maintained in the required platform state before the TOE performs authorisation acquisition or provides the resulting authorisation value to the Self-Encrypting Drive. Administrators must not modify the platform firmware, boot configuration, power-state settings or other security-relevant configuration in a manner that places the TOE outside its evaluated configuration.

The TOE relies on complete removal of power to clear key material from volatile memory and return protected drives to a locked state. Administrators must therefore ensure that the host platform is fully shut down or transitioned into a

compliant power state when the TOE is no longer in use. Suspend, hibernation or other non-evaluated power states must not be used where those states do not provide the required key-destruction and drive-locking behaviour.

The Baseboard Management Controller (BMC) is used only during installation and initial configuration. Following completion of the image-loading and installation process, the BMC must be disconnected or otherwise rendered inaccessible in accordance with the security guidance. The BMC must not remain network-accessible during normal operation of the TOE. This restriction is necessary because the Baseboard Management Controller is outside the TOE boundary and is not included within the evaluated security functionality.

TOE software updates must be obtained through authorised distribution channels and verified using the evaluated trusted-update mechanism before installation. Administrators must ensure that the update bundle and corresponding verification key originate from an authorised source and must not install an update where signature verification, integrity verification or package validation fails.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the relevant *Protection Profile [4]* and *Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3 [1, 2].*

Testing methodology was drawn from *Common Methodology for Information Technology Security, April 2017 Version 3.1 Revision 5 [3]* and relevant *Supporting Documents [11].*

The evaluation was carried out in accordance with the operational procedures of the *Australian Information Security Evaluation Program [10]*.

In addition, the conditions outlined in the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security [9]* and the document *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs [12]* were also upheld.

Functional Testing

All functional tests performed by the evaluators were taken from the *Protection Profile [4]* and *Supporting Document [11].* The tests were designed to provide the required testing coverage for the security functions claimed by the TOE.

Penetration Testing

The evaluators performed the evaluation activities for vulnerability assessment specified by the *FDE cPP for the Authorization Acquisition Supporting Document [11]* that follow a flaw hypothesis methodology. Accordingly, four types of flaw hypotheses have been considered:

- Type 1 - public vulnerabilities
- Type 2 - international Technical Community (iTC) sourced
- Type 3 - evaluation team generated
- Type 4 - tool generated.

The evaluators conducted a review of public vulnerability databases and technical community sources to determine potential flaw hypotheses using searches that include TOE device name and components, protocols supported by the TOE and terms relating to the device type of the TOE. These searches were conducted up to the 22 July 2026 coinciding with the conclusion of the evaluation. There were three identifiable Type 2 hypotheses for this evaluation, one applicable to the TOE.

The evaluators performed the following tests to discover any potential vulnerabilities of the TOE:

- Performing a vulnerability scan on the TOE

- Analysis of the BMC and RHEL interfaces, including tool-generated packet fuzzing vulnerability testing of the TOE as per the *Supporting Document [11].*

- Testing of the SED authentication sequence

Based on the results of this testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

This certification is focused on the evaluation of product compliance with Protection Profiles that cover the technology area of Full Drive Encryption Authorisation Acquisition. Organisations can have confidence that the scope of an evaluation against an ASD-approved Protection Profile covers the necessary security functionality expected of the evaluated product and known threats will have been addressed.

The analysis is supported by testing as outlined in the *PP Supporting Document [11]* and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with the *Protection Profile (PP) [4].* PP provide assurance by providing a full Security Target, and an analysis of the Security Functional Requirements in that *Security Target [8], guidance documentation [6],* and a basic description of the architecture of the TOE.

Certification Result

Teron Labs **has determined** that the TOE upholds the claims made in the *Security Target [8]* and **has met** the requirements of the Protection Profile *CPP_FDE_AA_V2.0E [4].*

After due consideration of the conduct of the evaluation as reported to the certifiers, and of *the Evaluation Technical Report [7]*, the Australian Certification Authority **certifies** the evaluation of the RackTop SHIELD v1.0 performed by the Australian Information Security Evaluation Facility, Teron Labs.

The Australian Certification Authority certifies that the *Security Target [8]* have met the requirements of the FDE AA *Protection Profile [4].*

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian Government users. For further guidance, Australian Government users should refer to the *Australian Government Information Security Manual [5].*

In addition to ensuring that the assumptions concerning the operational environment are fulfilled, and the guidance document is followed, the Australian Certification Authority also recommends that users and administrators:

- The users should make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings.
- Users of the TOE shall ensure that the BMC functionality is disabled following the setup of the TOE, per section 2.2.1 of the *guidance document [6].*

- Users to note that installation of the TOE image is only possible through the BMC, the product environment during the process of installation is not considered a CC compliant environment.
- Users of the TOE shall be aware that losing the PIN files or the USB they are stored on will lead to complete loss of access to data on the TOE.
- Once SEDs unlocked, the use of SSH may be used via the inner layer RHEL OS, however no assurance is provided for this functionality.

Annex – References and Abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5*
2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*
3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*
4. *collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, 01 February 2019 (CPP_FDE_AA_V2.0E)*
5. *Australian Government Information Security Manual: https://www.cyber.gov.au/ism*
6. *RackTop Systems Inc. RackTop SHIELD v1.0 Guidance Supplement, Version 0.8, 21 September 2026.*
7. *Evaluation Technical Report RackTop SHIELD v1.0 Version 1.0, dated 09 October 2026 (Document reference EFT-T067-ETR 1.0)*
8. *Security Target RackTop Systems, Inc. RackTop SHIELD v1.0, version 1.2, 06 October 2026.*
9. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014*
10. *AISEP Policy Manual (APM): https://www.cyber.gov.au/sites/default/files/2023-03/2022_AUG_REL_AISEP_Policy_Manual_6.3.pdf*
11. *Protection Profile Supporting Documents Mandatory Technical Document, Full Drive Encryption: Authorization Acquisition, Version 2.0 + Errata 20190201, 01 February 2019 (CPP_FDE_AA_V2.0E_SD)*
12. *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs 30 September 2021, Version 2.0, CCDB-013-v2.0*
13. *National Security Agency, Commercial Solutions for Classified, Data at Rest Capability Packages: https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/capability-packages/ - data-at-rest*
14. *Australian Government ASD Essentials: https://www.cyber.gov.au/essentials*

Abbreviations

AISEP	Australian Information Security Evaluation Program
AA	Authorisation Acquisition
ACA	Australian Certification Authority
APM	AISEP Policy Manual
ASD	Australian Signals Directorate
BMC	Baseboard Management Controller
CC	Common Criteria
CEM	Common Methodology for Information Technology Security Evaluation
cPP	collaborative Protection Profile
CPU	Central processing unit
CSfC	Commercial Solutions for Classified
DAR	Data-at-Rest
ETR	Evaluation Technical Report
FDE	Full Drive Encryption
FIPS	Federal Information Processing Standard
GHz	Gigahertz
IT	Information Technology
iTC	international Technical Community
OS	Operating System
PDF	Portable Document Format
PP	Protection Profile
RHEL	Red Hat Enterprise Linux
SEDs	Self-encrypting drives
SSH	Secure Shell
SSL	Secure Sockets Layer
TB	Terabyte

TCG- Compliant	Trusted Computing Group Compliant
TOE	Target of Evaluation
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2026

With the exception of the Coat of Arms, the Australian Signals Directorate logo and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/government/commonwealth-coat-arms).

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)



Australian Government

Australian Signals Directorate