Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

HPE Aruba Networking Virtual Intranet Access (VIA) Client version 4.7

Version 1.01, 14 October 2026

Document reference: AISEP-CC-CR-2026-EFT-T050-CR-v1.01
(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 6

Secure Delivery 6

Version Verification 7

Documentation and Guidance 7

Secure Usage 7

Evaluation **9**

Overview 9

Evaluation Procedures 9

Functional Testing 9

Entropy Testing 9

Penetration Testing 9

Software Bill of Material (SBOM) assessment 9

Certification **11**

Overview 11

Assurance 11

Certification Result 11

Recommendations 11

Annex – References and Abbreviations 13

References 13

Abbreviations 14

Executive Summary

This report describes the findings of the IT security evaluation of HPE Aruba Networking Virtual Intranet Access (VIA) Client version 4.7 developed by HPE Aruba Networking against Common Criteria approved Protection Profiles (PPs).

The Target of Evaluation (TOE) is the HPE Aruba Virtual Intranet Access (VIA) Client version 4.7. The TOE is a software application with IPsec VPN client capability.

This report concludes that the TOE has complied with the following *PPs [4]:*

- *Protection Profile for Application Software, version 1.4, 07 October 2021 (PP_APP_V1.4)*
- *PP-Module for Virtual Private Network (VPN) Clients, version 2.4, 31 March 2022 (MOD_VPNC_V2.4)*

Additionally, the above PPs can be grouped together using certified PP-Configuration. This evaluation used the following *PP-Configuration [4]:*

- *PP-Configuration for Application Software and Virtual Private Network (VPN) Clients, Version 1.3, 07 April 2023 (CFG_APP-VPNC_V1.3)*

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) submitted on 10 July 2026.

With regard to the secure operation of the TOE, the Australian Certification Authority recommends that:

- Potential users of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.
- The users should make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings.
- The system auditor should review the audit trail generated and exported by the TOE periodically.

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 Profiles [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 the HPE Aruba Networking Virtual Intranet Access (VIA) Client version 4.7 developed by HPE Aruba Networking.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	HPE Aruba Networking Virtual Intranet Access (VIA) Client version 4.7
Software version	4.7
Security Target	HPE Aruba Networking Virtual Intranet Access (VIA) Client Version 4.7 Security Target, Version 1.0.2, 08 October 2026
Evaluation Technical Report	Evaluation Technical Report 1.0, dated 10 July 2026 Document reference EFT-T050-ETR 1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Extended, April 2017, Version 3.1 Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5
Conformance	▪ Protection Profile for Application Software, version 1.4, 07 October 2021 (PP_APP_V1.4) ▪ PP-Module for Virtual Private Network (VPN) Clients, version 2.4, 31 March 2022 (MOD_VPNC_V2.4)

	▪ PP-Configuration for Application Software and Virtual Private Network (VPN) Clients, Version 1.3, 07 April 2023 (CFG_APP-VPNC_V1.3)
Developer	HPE Aruba Networking 11445 Compaq Centre Drive West Houston 77070 TX USA
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 the HPE Aruba Networking Virtual Intranet Access (VIA) Client version 4.7, a non-distributed VPN client application that enables remote and mobile users to securely access enterprise network resources over untrusted networks. Installed on end-user devices, the TOE authenticates users through a Mobility Controller-hosted gateway, retrieves connection policies and configuration profiles, and establishes a secure IPsec VPN tunnel to enterprise resources. The TOE uses HTTPS to communicate with the gateway for authentication and configuration download, and IPsec/IKE over UDP port 4500 to provide protected communications. By enforcing secure remote connectivity and policy-based access to enterprise networks, the TOE supports trusted access to organisational resources from external locations.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.4 of the *Security Target [8].*

TOE Physical Boundary

The physical boundary of the TOE includes the HPE Aruba Networking Virtual Intranet Access (VIA) Client version 4.7 software application, the supported operating system platforms on which it executes, the evaluated hardware platforms used during testing, and the associated security guidance documentation. The TOE is a software-only VPN client that operates on general-purpose computing and mobile device hardware. The components included within the TOE physical boundary are detailed in *Table 1*.

Part of the TOE	Identification	Description
TOE Software (Windows)	Aruba-VIA-4.7.6.0.2603183-64.msi	VIA Client v4.7 VPN client software running on Microsoft Windows 11 (64-bit).
TOE Software (Linux)	cc-via_4.7.6.2603081-deb_amd64.deb	VIA Client v4.7 VPN client software running on Ubuntu 24.04.
TOE Software (Android)	HPE-VIA-4.7.5.2603170.apk	VIA Client v4.7 VPN client software running on Android 14.
Security Guidance	Guidance Document, Aruba Virtual Intranet Access (VIA) 4.x Client Common Criteria Guidance, Version 2.5	The Common Criteria Guidance supplement for the TOE. The security guidance is distributed as a document in PDF format.
Product Documentation	https://arubanetworking.hpe.com/techdocs/VIA/HPE-Aruba-VIA/Content/home.htm	Supporting product documentation available from the HPE Aruba Networking documentation portal.

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

Architecture

The TOE provides secure connectivity for users when accessing an enterprise or corporate resource (example: workstation, server) from an untrusted or trusted network connection. By default, the TOE automatically launches and establishes a remote connection when the user logs in to their system from an untrusted network.

The TOE runs on an end-user device and communicates with a gateway located on a Mobility Controller. The server component is used to manage the client and ensure policies are enforced. The Mobility Controller maintains certain VIA configuration profiles, such as the VIA authentication profile, the VIA connection profile, and the VIA web authentication profile. Each profile plays an important role in authenticating the users and establishing a secure connection. When multiple authentication profiles are available, the VIA client prompts the user to select an authentication profile.

The first time a connection is established, a user opens the VIA client and enters the gateway name, username, and password. VIA then connects to the gateway over an HTTPS channel and attempts to authenticate using the user supplied credentials. The TSF relies on the underlying OS platform for establishment of the HTTPS channel; it is not part of the TOE itself. This connection is used to retrieve configuration settings for the IPsec connection and any site-specific branding (e.g. logo graphics).

If the VIA web authentication list has more than one VIA authentication profile, the user can choose a VIA authentication profile from the available ones. After successful authentication, the VIA client downloads the appropriate VIA connection profile and establishes the IPsec connection if the user is connected to an untrusted network.

At a protocol level, VIA operates over UDP port 4500, which is defined for IKE/IPsec traversal of NATs in RFC 3947. VIA uses HTTPS over TCP port 443 in order to contact the authentication server and download configuration profile updates before establishing each IKE/IPsec connection. The VIA topography is shown in the *Figure 1* below.

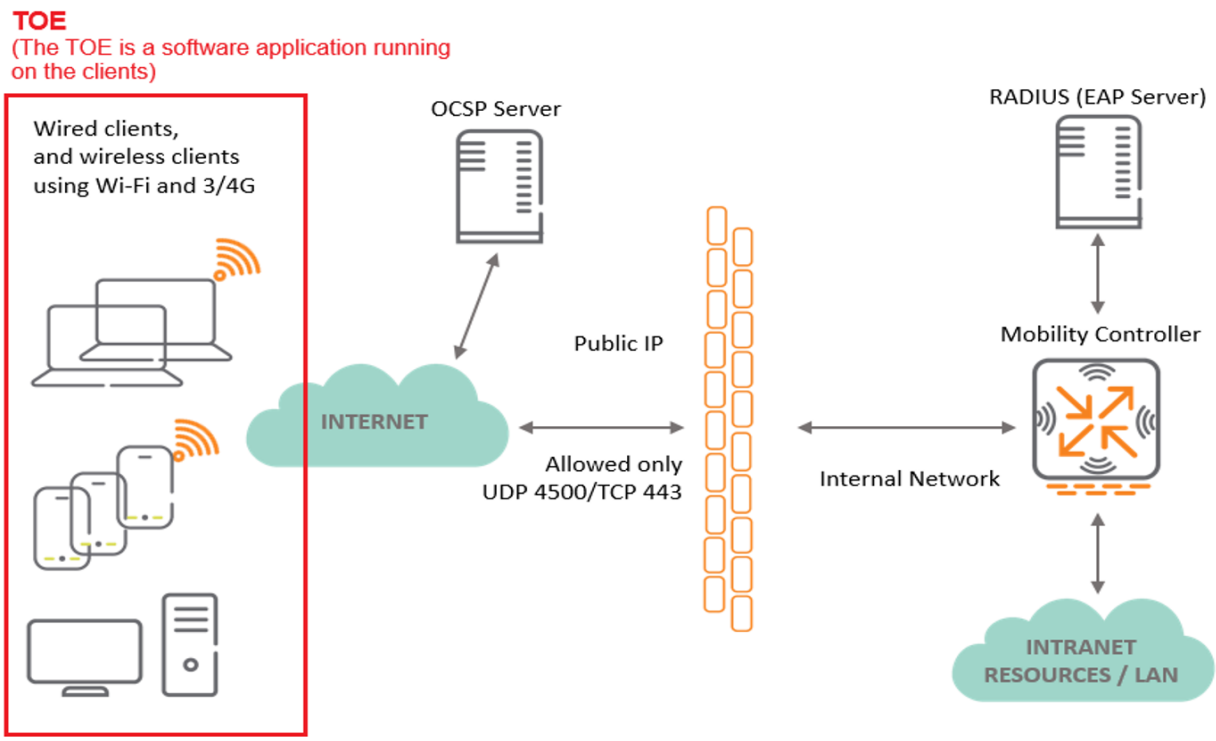

Figure 1. TOE Architecture

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 Profiles [4]* and *Supporting Documents [12]* 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 IPsec VPN client. 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.

- An OCSP server is required for the TOE to be able to perform certificate validation.
- The Mobility Controller is required in the operational environment because the TOE uses it as its VPN gateway. The VIA client can work in the evaluated configuration with the Mobility Controller running ArubaOS 8.13 from 8.13.1 and later, but has only been tested with ArubaOS 8.13.1.
- An EAP server (such as a RADIUS server) may or may not be used for authentication.
- The HP ProBook 440 G11 with Intel Core Ultra 7 155U platform was used by the evaluator for testing the Windows and Linux supported platform of the TOE, and the Samsung Galaxy S24 was used by the evaluator for testing the Android supported platform of the TOE. This hardware and hosting operating system is not part of the TOE.

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 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 HPE Aruba Networking Support Portal.

The Linux and Windows versions of the TOE can be downloaded by registered customers from the HPE Networking Support Portal; per-platform instructions are present in the *Configuration Guidance [6]*. The Android version can be installed using the Google Play Store. These mechanisms are also used for the deployment of security updates.

Installation of the TOE

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

Version Verification

The TOE may be installed by the platform administrator on each supported platform. For the Linux and Windows versions of the TOE, the TOE verification is performed automatically by their respective installers using an RSA 2048 digital signature with SHA-1, signed by HPE Aruba Networking. A successful installation process indicates that this check succeeded. The Android version of the TOE is verified by the Android platform when it is installed through the Google Play Store, using an RSA 2048 bit with SHA-256 digital signature.

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 titled as:

- *Guidance Document, Aruba Virtual Intranet Access (VIA) 4.x Client Common Criteria Guidance, Version 2.5*

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].*

Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

The application software is assumed to be physically secured within its operational environment, protected from physical attacks that could compromise its security or interfere with its physical connections and correct operation. This level of protection is expected to be sufficient to safeguard the device and the sensitive data it handles.

The TOE is designed to provide Virtual Private Network (VPN) client functionality. It must not be used as a general-purpose computing platform, nor should it support activities such as executing compilers, running arbitrary user applications, or performing functions unrelated to its defined networking and security role. Restricting the TOE to its intended purpose ensures that its operational behaviour remains predictable and that its security controls cannot be undermined by unauthorised or non-security-related functionality.

The administrator(s) are assumed to be trustworthy, acting in the best interests of the organisation's security. This includes being well-trained, adhering to established policies, and following all guidance documentation. Administrators are responsible for ensuring that passwords and credentials used within the TOE are strong and secure. The TOE is not expected to protect against a malicious administrator who deliberately seeks to bypass or compromise its security features.

For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

The TOE is assumed to be connected to distinct networks in a way that ensures its security policies are enforced on all relevant network traffic flowing between these networks.

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 Profiles [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 [12].*

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 [13]* were also upheld.

Functional Testing

All functional tests performed by the evaluators were taken from the *Protection Profiles [4]* and *Supporting Documents [12].* The tests were designed to provide the required testing coverage for the security functions claimed by the TOE.

Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate *report [11]*.

Penetration Testing

The evaluators performed the evaluation activities for vulnerability assessment specified by the *Protection Profile for Application Software [4.a]*.

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 02 June 2026 coinciding with the conclusion of the evaluation.

Software Bill of Material (SBOM) assessment

As part of the requirements outlined in the NIAP Policy Letter #30, the evaluator also submitted the TOE's Software Bill of Materials (SBOM). The SBOM provides a comprehensive inventory of all software components, third-party libraries, and dependencies included within the evaluated TOE. Submission of this information enables supply-chain

integrity verification, supports systematic vulnerability correlation across all embedded components, and ensures that no undeclared software elements are present within the TOE. *The SBOM Analysis report [14]* contains the minimum elements as adapted from the National Telecommunications and Information Administration (NTIA) and serves as an essential artefact informing the vulnerability assessment activities and contributes materially to the assurance gained through the evaluation process.

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 application software with added security functionality including VPN Client functions. 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 Documents and Protection Profile Module activities, SBOM assessment, 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 Profiles (PPs) [4].* PPs provide assurance by providing a full *Security Target [8]*, and an analysis of the Security Functional Requirements in that Security Target, guidance documentation, 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 Profiles *PP_APP_V1.4 [4.a], MOD_VPNC_V2.4 [4.b]* and *PP configuration for Application Software and Virtual Private Network (VPN) Clients [4.c]*.

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 HPE Aruba Networking Virtual Intranet Access (VIA) Client version 4.7 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 Application Software and VPN Client *Protection Profiles [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:

- Potential users of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.
- The users should make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings.

- The system auditor should review the audit trail generated and exported by the TOE periodically.

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. Protection Profiles:

   a) *Protection Profile for Application Software: v1.4, 7 October 2021 (PP_APP_V1.4)*

   b) *Protection Profile Module for VPN Client: v2.4, 31 March, 2022 (MOD_VPNC_V2.4)*

   c) *PP-Configuration for Application Software and Virtual Private Network (VPN) Clients, Version 1.3, 07 April 2023 (CFG_APP-VPNC_V1.3)*

5. *Australian Government Information Security Manual: https://www.cyber.gov.au/ism*

6. *Aruba Virtual Intranet Access (VIA) 4.x Client Common Criteria Guidance, Version 2.5, dated July 2026*

7. *Evaluation Technical Report, HPE Aruba Virtual Intranet Access (VIA) Client version 4.7, Version 1.0, dated 10 July 2026* (Document reference EFT-T050-ETR 1.0)

8. *Security Target, HPE Aruba Networking Virtual Intranet Access (VIA) Client Version 4.7 Security Target, Version 1.0.2, 08 October 2026.*

9. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 02 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. Entropy Documentation:

    a) *Entropy Assessment Report, HPE Aruba Networking Virtual Intranet Access (VIA) Client Version 4.7 Version 1.0, Dated 09 July 2026 (Document reference EFT-T050-EAR 1.0)*

12. Protection Profile Supporting Documents

    a) *Supporting Document Mandatory Technical Document for PP-Module for Virtual Private Network (VPN) Clients, Version 2.4, 31 March 2022*

13. *CC and CEM Addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs, Version 2.0, 30 September 2021, CCDB-013-v2.0*

14. *SBOM Analysis report, HPE Aruba Virtual Intranet Access (VIA) Client Version 4.7, Version 1.0, dated 06 August 2026*

Abbreviations

AISEP	Australian Information Security Evaluation Program
ASD	Australian Signals Directorate
CA	Certificate Authority
CCRA	Common Criteria Recognition Arrangement
EAP	Extensible Authentication Protocol
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange Version 2
IPsec	Internet Protocol Security
LAN	Local Area Network
NAT	Network Address Translation
NGC	Northrop Grumman Corporation
OCSP	Online Certification Status Protocol
OS	Operating System
PP	Protection Profile
SBOM	Software Bill of Materials
SSH	Secure Shell
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TLS	Transport Layer Security
UDP	User Datagram Protocol
VIA	Virtual Intranet Access
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

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