Content changes

Guidelines for cyber security incidents

- Security control 0122 was removed due to being a duplication of the intent of security control 0043.
- Minor amendment to fix the reference to the System-specific security documentation section.
- Amendments to ‘Reporting cyber security incidents to the ACSC’ content.
- Security control 0140 was updated.

Guidelines for security documentation

- Amendments to ‘Security documentation’ content.
- Reintroduction of security control 0039.
- Amendments to ‘Approval of security documentation’.
- Security control 0047 was updated to include organisational-level security documentation within its scope.
- Amendments to ‘Maintenance of security documentation’ content.
- Security control 0888 was updated to include organisational-level security documentation within its scope.

Guidelines for media management

- Security control 0338 was removed due to being a duplication of the intent of security control 0161.

Guidelines for network management

- Security control 0576 was moved to the Detecting cyber security incidents section of the Guidelines for cyber security incidents.

Guidelines for using cryptography

- ‘Suite B’ content was removed.
- ‘Commercial National Security Algorithm Suite’ content was removed.
- ‘Selecting cryptographic algorithms’ content was removed.
Amendments were made to ‘Protecting highly classified information’ content.

Security control 1232 was updated to remove references to Suite B and CNSA Suite algorithms.

Security control 1468 was updated to include key sizes.

Guidelines for data transfers and content filtering

Security control 0665 was updated to remove the requirement for a formal risk assessment. This ensures consistency with other circumstances in which a Chief Information Security Officer (CISO) may delegate duties.

Security assessment aids

Security control 0140 was updated to reflect changes made to the Guidelines for cyber security incidents.

Security controls 0039, 0047 and 0888 were updated to reflect changes made to the Guidelines for security documentation.

Security control 1112 in the Guidelines for communications infrastructure was updated to reflect the correct content from the source document.

Security control 0576 was moved from the Guidelines for network management to the Guidelines for cyber security incidents.

Security controls 1232 and 1468 were updated to reflect changes made to the Guidelines for using cryptography.

Security control 0665 was updated to reflect changes made to the Guidelines for data transfers and content filtering.

List of modified security controls

Security Control: 0140; Revision: 6; Updated: May-19; Applicability: O, P, S, TS; Priority: Must
Cyber security incidents are reported to the ACSC.

Security Control: 0039; Revision: 4; Updated: May-19; Applicability: O, P, S, TS; Priority: Must
A cyber security strategy is developed and implemented for the organisation.

Security Control: 0047; Revision: 4; Updated: May-19; Applicability: O, P, S, TS; Priority: Should
Organisational-level security documentation is approved by the Chief Information Security Officer while system-specific security documentation is approved by the system’s authorising officer.

Security Control: 0888; Revision: 5; Updated: May-19; Applicability: O, P, S, TS; Priority: Should
Security documentation is reviewed at least annually and includes a ‘current as at [date]’ or equivalent statement.

Security Control: 1232; Revision: 5; Updated: May-19; Applicability: S, TS; Priority: Must
AACAs are used in an evaluated implementation.

Security Control: 1468; Revision: 4; Updated: May-19; Applicability: S, TS; Priority: Should
Preference is given to using the CNSA Suite algorithms and key sizes where possible.

Security Control: 0665; Revision: 4; Updated: May-19; Applicability: S, TS; Priority: Must
Trusted sources are a strictly limited number of personnel that have been authorised as such by an organisation’s CISO.