Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

JUNE 2021

Guidelines for Communications Infrastructure

Cabling infrastructure

Applicability

The security controls in this section apply to new cabling infrastructure installations or upgrades. Organisations do not need to retrofit existing cabling infrastructure to align with these security controls.

This section is applicable to all domestic facilities. For deployable platforms or facilities outside of Australia, consult the emanation security section of these guidelines.

Implementation scenarios

This section provides common security controls for non-shared government facilities, shared government facilities and shared non-government facilities:

- A non-shared government facility is where the entire facility and personnel are cleared to the highest level of data processed in the facility.
- A shared government facility is where the facility and personnel are cleared at different levels.
- A shared non-government facility is where the facility is shared by government organisations and non-government organisations.

Specific security controls for any of the above scenarios will be identified as such.

Cable sheaths and conduits

A cable’s protective sheath is not considered to be a conduit. However, for fibre-optic cables with subunits, the fibre-optic cable’s outer protective sheath is considered to be a conduit.

Cable connector types

The same cable connector types can be used for all systems within a facility regardless of their sensitivity or classification.

Cabling infrastructure standards

Cabling infrastructure should be installed by an endorsed cable installer to the relevant Australian Standards to ensure personnel safety and system availability.

Security Control: 0181; Revision: 3; Updated: Mar-21; Applicability: O, P, S, TS
Cabling infrastructure is installed in accordance with relevant Australian Standards, as directed by the Australian Communications and Media Authority.

Use of fibre-optic cables

Fibre-optic cables do not produce, nor are influenced by, electromagnetic emanations; thereby offering the highest degree of protection from electromagnetic emanation effects. Also, fibre-optic cables are more difficult to tap than copper cables.

Security Control: 1111; Revision: 3; Updated: Mar-21; Applicability: O, P, S, TS
Fibre-optic cables are used for cabling infrastructure instead of copper cables.

Cable register

Maintaining and regularly auditing cable registers assists installers and inspectors, with the help of floor plan diagrams, to trace cables for malicious or accidental changes or damage. In doing so, cable registers should track all cabling changes throughout the life of a system.

Security Control: 0211; Revision: 5; Updated: Jan-21; Applicability: O, P, S, TS
A cable register is maintained and regularly audited.

Security Control: 0208; Revision: 6; Updated: Jun-21; Applicability: O, P, S, TS
A cable register contains the following for each cable:

- *cable identifier*
- *cable colour*
- *sensitivity/classification*
- *source*
- *destination*
- *location*
- *seal numbers (if applicable).*

Floor plan diagrams

Floor plan diagrams, developed using computer-aided design and drafting software, providing an accurate scaled view for each floor and using alphanumeric grid referencing, are critical to ensuring that cabling infrastructure components can be easily located by installers and inspectors. In doing so, floor plan diagrams should track all cabling infrastructure changes throughout the life of a system.

Security Control: 1645; Revision: 0; Updated: Jun-21; Applicability: O, P, S, TS
Floor plan diagrams are maintained and regularly audited.

Security Control: 1646; Revision: 0; Updated: Jun-21; Applicability: O, P, S, TS
Floor plan diagrams contain the following:

- *cable paths (including ingress and egress points between floors)*
- *cable reticulation system and conduit paths*
- *floor concentration boxes*
- *wall outlet boxes*
- *network cabinets.*

Cable labelling process and procedures

A well documented and followed cable labelling process, and supporting cable labelling procedures, makes cable auditing and fault finding easier.

Security Control: 0206; Revision: 5; Updated: Aug-19; Applicability: O, P, S, TS
A cable labelling process, and supporting cable labelling procedures, is developed and implemented.

Labelling cables

Labelling cables with the correct source and destination details minimises the likelihood of cross-patching and aids in fault finding and configuration management.

Security Control: 1096; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
Cables are labelled at each end with sufficient source and destination details to enable the physical identification and inspection of the cable.

Labelling building management cables

All facilities will contain cabling to support building management functions, such as: security systems, fire detection systems, building management systems, audio/visual systems, operational technology sensors and lighting. As building management cables may use colours such as red for fire alarms (as per Australian Standards), it is important that such cables are appropriately labelled.

Security Control: 1639; Revision: 0; Updated: Mar-21; Applicability: O, P, S, TS
Building management cables are labelled with their purpose in black writing on a yellow background, with a minimum size of 2.5 cm x 1 cm, and attached at five-metre intervals.

Labelling cables for foreign systems in Australian facilities

Labelling cables for foreign systems in Australian facilities helps prevent unintended cross-patching of Australian and foreign systems.

Security Control: 1640; Revision: 0; Updated: Mar-21; Applicability: O, P, S, TS
Cables for foreign systems installed in Australian facilities are labelled at inspection points.

Cable colours

The use of designated cable colours can provide an easy way to distinguish highly classified systems from other systems. For example, while TOP SECRET and SECRET cables have designated colours, cables for PROTECTED and below systems may be any colour (except for those reserved for highly classified systems). In addition, cable colours for PROTECTED and below systems may be the same colour (e.g. blue).

Security Control: 0926; Revision: 8; Updated: Mar-21; Applicability: O, P, S, TS
The cable colours in the following table are used.

System	***Cable Colour***
TOP SECRET	*Red*
SECRET	*Salmon pink*
PROTECTED	*Any colour (except red or salmon pink)*

OFFICIAL	*Any colour (except red or salmon pink)*

Cable colour non-conformance

In certain circumstances it may not be possible to use the correct cable colours. Therefore, organisations should band cables with the appropriate colour and ensure that the cable bands are easily visible at inspection points. In doing so, it is important that cable bands are robust enough to stand the test of time. Examples of appropriate cable bands include stick-on coloured labels, colour heat shrink, coloured ferrules or short lengths of banded conduit.

Security Control: 1216; Revision: 2; Updated: Mar-21; Applicability: S, TS
Cables with non-conformant cable colouring are both banded with the appropriate colour and labelled at inspection points.

Cable inspectability

The ability to inspect cabling infrastructure is necessary to detect illicit tampering or degradation.

Security Control: 1112; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
In non-shared government facilities, cables are inspectable at a minimum of five-metre intervals.

Security Control: 1118; Revision: 1; Updated: Sep-18; Applicability: O, P, S
In non-TOP SECRET areas of shared government facilities, cables are inspectable at a minimum of five-metre intervals.

Security Control: 1119; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
In TOP SECRET areas of shared government facilities, cables are fully inspectable for their entire length.

Security Control: 1126; Revision: 1; Updated: Sep-18; Applicability: O, P, S
In non-TOP SECRET areas of shared non-government facilities, cables are inspectable at a minimum of five-metre intervals.

Security Control: 0184; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
In TOP SECRET areas of shared non-government facilities, cables are fully inspectable for their entire length.

Cable groups

Cable groups provide a method of sharing conduits and cable reticulation systems.

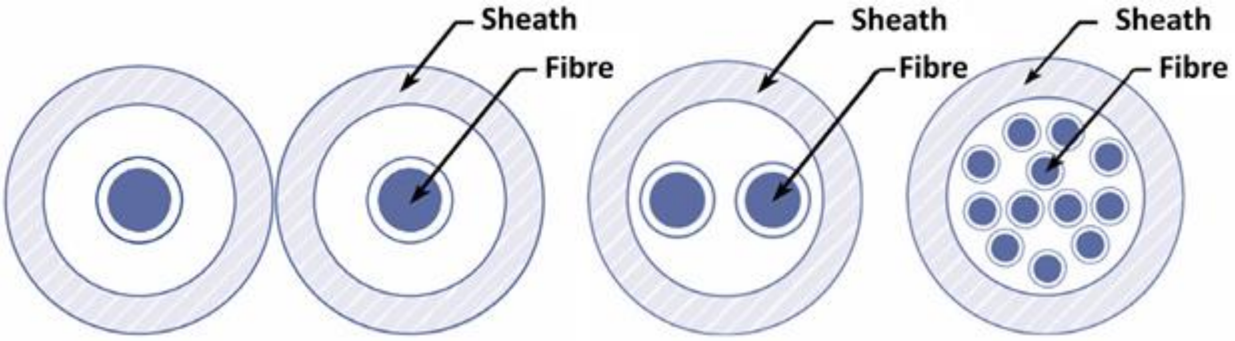
Security Control: 0187; Revision: 6; Updated: Mar-21; Applicability: O, P, S, TS
The cable groups in the following table are used.

Cable Group	***System***
1	*OFFICIAL*
	PROTECTED
2	*SECRET*
3	*TOP SECRET*

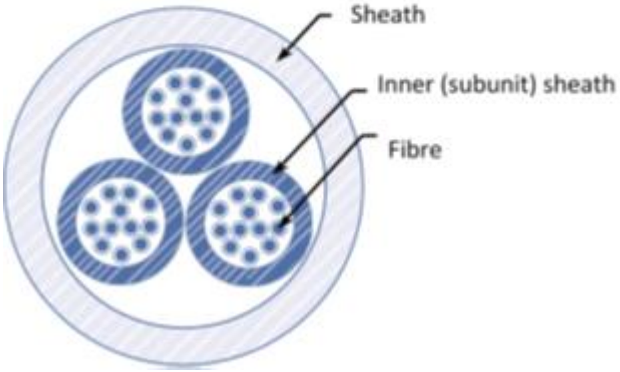
Fibre-optic cables sharing a common conduit

Fibre-optic cables of various cable groups can share a common conduit to reduce costs; however, various cable groups can’t share a common sheath unless they belong to different subunits.

Security Control: 0189; Revision: 3; Updated: Mar-21; Applicability: O, P, S, TS
With fibre-optic cables, the fibres in the sheath only carry a single cable group.



Security Control: 0190; Revision: 3; Updated: Mar-21; Applicability: O, P, S, TS
With fibre-optic cables contains subunits, each subunit only carries a single cable group; however, each subunit can carry a different cable group.



Common cable reticulation systems

Laying cables in a neat and controlled manner that allows for inspection reduces the need for individual cable trays.

Security Control: 1114; Revision: 3; Updated: Mar-21; Applicability: O, P, S, TS
Cable groups sharing a common cable reticulation system have a dividing partition or a visible gap between the cable groups.

Enclosed cable reticulation systems

In shared non-government facilities, cables should be enclosed in a sealed cable reticulation system to prevent access and enhance cable management.

Security Control: 1130; Revision: 3; Updated: Oct-19; Applicability: O, P, S, TS
In shared non-government facilities, cables are run in an enclosed cable reticulation system.

Covers for enclosed cable reticulation systems

In shared non-government facilities, clear covers on enclosed cable reticulation systems are a convenient method of maintaining inspection requirements. Having clear covers face inwards increases their inspectability.

Security Control: 1164; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
In shared non-government facilities, conduits or the front covers of ducts, cable trays in floors and ceilings, and associated fittings are clear plastic.

Sealing cable reticulation systems and conduits

In shared non-government facilities, Security Construction and Equipment Committee (SCEC) endorsed seals should be used to provide evidence of any tampering or illicit access to cable reticulation systems. In addition, conduits should be sealed with a visible smear of conduit glue to prevent access.

Security Control: 0195; Revision: 5; Updated: Mar-21; Applicability: TS
In shared non-government facilities, uniquely identifiable SCEC endorsed tamper-evident seals are used to seal all removable covers on cable reticulation systems.

Security Control: 0194; Revision: 2; Updated: Sep-18; Applicability: TS
In shared non-government facilities, a visible smear of conduit glue is used to seal all plastic conduit joints and conduit runs connected by threaded lock nuts.

Labelling conduits

Conduit labels should be a specific size and colour to allow for easy identification.

Security Control: 0201; Revision: 3; Updated: Mar-21; Applicability: TS
Labels for TOP SECRET conduits are a minimum size of 2.5 cm x 1 cm, attached at five-metre intervals and marked as 'TS RUN'.

Cables in walls

Cables run correctly in walls allow for neater installations while maintaining separation and inspection requirements.

Security Control: 1115; Revision: 4; Updated: Dec-19; Applicability: O, P, S, TS
Cables from cable trays to wall outlet boxes are run in flexible or plastic conduit.

Cables in party walls

In shared non-government facilities, cables should not be run in any wall shared with an unsecured space where there is no control over access. An inner wall can be used to run cables where the space is sufficient for inspection of the cables.

Security Control: 1133; Revision: 2; Updated: Mar-21; Applicability: TS
In shared non-government facilities, cables are not run in party walls.

Wall penetrations

In shared government facilities and shared non-government facilities, penetrating a wall into a lower classified space requires the integrity of the classified spaces to be maintained. As such, all cables should be encased in conduit with no gaps in the wall around the conduit.

Security Control: 1122; Revision: 1; Updated: Sep-18; Applicability: TS
In shared government facilities, where wall penetrations exit into a lower classified space, cables are encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.

Security Control: 1134; Revision: 1; Updated: Sep-18; Applicability: TS
In shared non-government facilities, where wall penetrations exit into a lower classified space, cables are encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.

Wall outlet boxes

Wall outlet boxes are the main method of connecting cabling infrastructure to workstations. They allow the management of cables and the selection of the type of connectors allocated to various systems.

Security Control: 1104; Revision: 3; Updated: Mar-21; Applicability: O, P
Wall outlet boxes have connectors on opposite sides of the wall outlet box if the cable group contains cables belonging to different classifications.

Security Control: 1105; Revision: 3; Updated: Mar-21; Applicability: O, P, S, TS
Different cables groups do not share a wall outlet box.

Labelling wall outlet boxes

Clear labelling of wall outlet boxes diminishes the possibility of incorrectly attaching ICT equipment of a lower classification to the wrong wall outlet box. In cases were a wall outbox has a cable group containing cables belonging to different classifications, each connector should be individually labelled with its classification.

Security Control: 1095; Revision: 4; Updated: Mar-21; Applicability: O, P, S, TS
Wall outlet boxes denote the classifications, cable identifiers and wall outlet box identifier.

Wall outlet box colours

The use of designated wall outlet box colours can provide an easy way to distinguish highly classified systems from other systems. For example, while TOP SECRET and SECRET wall outlet boxes have designated colours, wall outlet boxes for PROTECTED and below systems may be any colour (except for those reserved for highly classified systems). In addition, wall outlet box colours for PROTECTED and below systems may be the same colour (e.g. white). Ideally, wall outlet boxes should be the same colour that is used for associated cabling infrastructure.

Security Control: 1107; Revision: 4; Updated: Mar-21; Applicability: O, P, S, TS
The wall outlet box colours in the following table are used.

System	***Wall Outlet Box Colour***
TOP SECRET	*Red*
SECRET	*Salmon pink*
PROTECTED	*Any colour (except red or salmon pink)*
OFFICIAL	*Any colour (except red or salmon pink)*

Wall outlet box covers

Transparent wall outlet box covers allow for inspection of cable cross-patching and tampering.

Security Control: 1109; Revision: 3; Updated: Dec-19; Applicability: O, P, S, TS
Wall outlet box covers are clear plastic.

Fly lead installation

Keeping the lengths of fibre-optic fly leads to a minimum prevents clutter around desks, prevents damage, and reduces the chance of cross-patching and tampering. If lengths become excessive, fly leads should be treated as cabling infrastructure and run in a conduit or fixed infrastructure such as desk partitioning.

Security Control: 0218; Revision: 5; Updated: Mar-21; Applicability: TS
If fibre-optic fly leads exceeding five metres in length are used to connect wall outlet boxes to ICT equipment, they are run in a protective and easily inspected pathway that is clearly labelled at the ICT equipment end with the wall outlet box's identifier.

Connecting cable reticulation systems to cabinets

Controlling the routing from cable management systems to cabinets can assist in preventing unauthorised modifications and tampering while also providing easy inspection of cables.

Security Control: 1102; Revision: 2; Updated: Mar-21; Applicability: O, P, S
In non-TOP SECRET areas, cable reticulation systems leading into cabinets are terminated as close as possible to the cabinet.

Security Control: 1101; Revision: 2; Updated: Mar-21; Applicability: O, P, S, TS
In TOP SECRET areas, cable reticulation systems leading into cabinets in a secure communications or server room are terminated as close as possible to the cabinet.

Security Control: 1103; Revision: 2; Updated: Mar-21; Applicability: O, P, S, TS
In TOP SECRET areas, cable reticulation systems leading into cabinets not in a secure communications or server room are terminated at the boundary of the cabinet.

Terminating cables in cabinets

Having individual or divided cabinets can assist in preventing accidental or deliberate cross-patching and makes inspection of cables easier.

Security Control: 1098; Revision: 3; Updated: Mar-21; Applicability: O, P, S
Cables are terminated in individual cabinets; or for small systems, one cabinet with a division plate to delineate cable groups.

Security Control: 1100; Revision: 1; Updated: Sep-18; Applicability: TS
TOP SECRET cables are terminated in an individual TOP SECRET cabinet.

Terminating cable groups on patch panels

Terminating cable groups on different patch panels in cabinets can assist in preventing accidental or deliberate cross-patching and makes inspection of cables easier.

Security Control: 0213; Revision: 3; Updated: Mar-21; Applicability: O, P, S, TS
Different cable groups do not terminate on the same patch panel.

Physical separation of cabinets and patch panels

Physical separation between TOP SECRET systems and systems of lower classifications reduces the chance of cross-patching, thereby the possibility of unauthorised personnel gaining access to TOP SECRET systems.

Security Control: 1116; Revision: 3; Updated: Oct-19; Applicability: O, P, S, TS
There is a visible gap between TOP SECRET cabinets and cabinets of lower classifications.

Security Control: 0216; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
TOP SECRET and non-TOP SECRET patch panels are physically separated by installing them in separate cabinets.

Security Control: 0217; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Where spatial constraints demand patch panels of lower classifications than TOP SECRET be located in the same cabinet as a TOP SECRET patch panel:

- *a physical barrier in the cabinet is provided to separate patch panels*
- *only personnel holding a Positive Vetting security clearance have access to the cabinet*
- *approval from the TOP SECRET system's authorising officer is obtained prior to installation.*

Audio secure spaces

Audio secure spaces are designed to prevent audio conversations from being overheard. The Australian Security Intelligence Organisation (ASIO) should be consulted before any modifications are made to audio secure spaces.

Security Control: 0198; Revision: 2; Updated: Sep-18; Applicability: TS
When penetrating an audio secured space, ASIO is consulted and all directions provided are complied with.

Power reticulation

In both shared government facilities and shared non-government facilities with TOP SECRET systems, it is important that TOP SECRET systems have control over the power system to prevent denial of service by deliberate or accidental means.

Security Control: 1123; Revision: 2; Updated: Sep-18; Applicability: TS
In TOP SECRET areas of shared government facilities, a power distribution board with a feed from an Uninterruptible Power Supply is used to power all TOP SECRET ICT equipment.

Security Control: 1135; Revision: 1; Updated: Sep-18; Applicability: TS
In TOP SECRET areas of shared non-government facilities, a power distribution board with a feed from an Uninterruptible Power Supply is used to power all TOP SECRET ICT equipment.

Further information

Australian Standards for cables can be obtained from the Australian Communications and Media Authority at https://www.acma.gov.au/cabling-standards-and-regulations.

Further information on physical security for Security Zones and secure rooms can be found in the Attorney-General's Department's ***Protective Security Policy Framework***, ***Entity facilities*** policy, at https://www.protectivesecurity.gov.au/physical/entity-facilities/Pages/default.aspx.

Further information on endorsed seals for various sealing requirements is available in the SCEC's ***Security Equipment Evaluated Products List*** at https://www.scec.gov.au/catalogue.

Emanation security

Applicability

This section is only applicable to:

- organisations located outside of Australia
- facilities in Australia that have transmitters
- facilities that are shared with non-Australian government entities
- mobile platforms and deployable assets that process data.

Emanation security threat assessments in Australia

Obtaining current threat advice from the Australian Cyber Security Centre (ACSC) on potential adversaries, and applying the appropriate counter-measures, is vital to protecting systems from emanation security threats.

Security Control: 0247; Revision: 3; Updated: Sep-18; Applicability: S, TS
System owners deploying systems with Radio Frequency (RF) transmitters inside or co-located with their facility contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the emanation security threat assessment.

Security Control: 0248; Revision: 5; Updated: Sep-18; Applicability: O, P, S
System owners deploying systems with RF transmitters that will be co-located with systems of a higher classification contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the emanation security threat assessment.

Security Control: 1137; Revision: 2; Updated: Sep-18; Applicability: TS
System owners deploying systems in shared facilities with non-Australian government entities contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the emanation security threat assessment.

Emanation security threat assessments outside Australia

Fixed sites outside Australia, and deployed military platforms, are more vulnerable to emanation security threats. Failing to implement recommended counter-measures and standard operating procedures to reduce threats could result in the platform emanating compromising signals, which if intercepted and analysed, could lead to platform compromise with serious consequences.

Security Control: 0932; Revision: 5; Updated: Sep-18; Applicability: O, P
System owners deploying systems overseas contact the ACSC for emanation security threat advice and implement any additional installation criteria derived from the emanation security threat advice.

Security Control: 0249; Revision: 3; Updated: Sep-18; Applicability: S, TS
System owners deploying systems overseas contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the emanation security threat assessment.

Early identification of emanation security issues

It is important to identify the need for emanation security controls for a system early in the project life cycle as this can reduce costs for the project. Costs are much greater if changes have to be made once the system has been designed and deployed.

Security Control: 0246; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
An emanation security threat assessment is sought as early as possible in a project's life cycle as emanation security controls can have significant cost implications.

Industry and government standards

While ICT equipment in a TOP SECRET area in Australia may not need certification to TEMPEST standards, the ICT equipment still needs to meet applicable industry and government standards.

Security Control: 0250; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
ICT equipment in TOP SECRET areas meets industry and government standards relating to electromagnetic interference/electromagnetic compatibility.