



Information Security Manual

DECEMBER 2021

Guidelines for Communications Infrastructure

Cabling infrastructure

Applicability

This section is only applicable to facilities located within Australia. In addition, this section only applies to new cabling infrastructure installations or upgrades.

Shared facilities

In addition to common security controls, this section provides additional security controls for shared facilities (e.g. a single floor, or part of a floor, within a multi-tenanted building).

Cables and structured cabling systems

For the purposes of this section, a cable is defined as any fibre optic or copper material housed within a protective sheath for the purposes of transmitting data or control signals from one point in a facility to another. Each cable will form part of a structured cabling system and will need to comply with the Australian Standards associated with that system. In addition to network communications and data systems, some common building management structured cabling systems found within facilities are:

- fire control and sensor systems
- security control and surveillance systems
- lighting control systems
- access control systems
- voice and emergency telephony systems
- emergency control alert systems.

Cable sheaths and conduits

A cable's protective sheath is not 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: All

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.

Security Control: 1111; Revision: 3; Updated: Mar-21; Applicability: All

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: All

A cable register is maintained and regularly audited.

Security Control: 0208; Revision: 6; Updated: Jun-21; Applicability: All

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, and using alphanumeric grid referencing, provide an accurate scaled view for each floor and 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: All

Floor plan diagrams are maintained and regularly audited.

Security Control: 1646; Revision: 0; Updated: Jun-21; Applicability: All

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 processes and procedures

Well documented cable labelling processes, and supporting cable labelling procedures, can make cable auditing and fault finding easier.

Security Control: 0206; Revision: 6; Updated: Dec-21; Applicability: All

Cable labelling processes, and supporting cable labelling procedures, are 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: All

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 structured cabling systems to support building management and control functions. As Australian Standards require some structured cabling systems to use colours such as red (e.g. fire control systems), it is important that all cables are appropriately labelled.

Security Control: 1639; Revision: 0; Updated: Mar-21; Applicability: All

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: All

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 SECRET and TOP SECRET systems from other systems. For example, while SECRET and TOP SECRET cables have designated colours, cables for other systems may be any colour except for those reserved for SECRET and TOP SECRET systems. In addition, cable colours for other systems may be the same colour (e.g. blue).

Security Control: 0926; Revision: 9; Updated: Dec-21; Applicability: O, P

OFFICIAL and PROTECTED cables are coloured neither salmon pink nor red.

Security Control: 1718; Revision: 0; Updated: Dec-21; Applicability: S

SECRET cables colours are coloured salmon pink.

Security Control: 1719; Revision: 0; Updated: Dec-21; Applicability: TS

TOP SECRET cables colours are coloured red.

Cable colour non-conformance

In certain circumstances it may not be possible to use the correct colour for SECRET or TOP SECRET cables. Therefore, organisations should band such 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: 3; Updated: Dec-21; Applicability: S, TS

SECRET and TOP SECRET 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: 3; Updated: Dec-21; Applicability: All

Cables are inspectable at a minimum of five-metre intervals.

Security Control: 1119; Revision: 2; Updated: Dec-21; Applicability: O, P, S, TS

Cables in TOP SECRET areas are fully inspectable for their entire length.

Common cable reticulation systems and conduits

Cables from different cable groups can share common cable reticulation systems and conduits to reduce costs.

Security Control: 0187; Revision: 7; Updated: Dec-21; Applicability: S, TS

SECRET and TOP SECRET systems belong exclusively to their own cable groups.

Security Control: 0189; Revision: 4; Updated: Sep-21; Applicability: All

Cables only carry a single cable group, unless each cable group belongs to a different subunit.

Security Control: 1114; Revision: 3; Updated: Mar-21; Applicability: All

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 facilities, cables should be enclosed in a sealed cable reticulation system to prevent access and enhance cable management.

Security Control: 1130; Revision: 4; Updated: Dec-21; Applicability: All

In shared facilities, cables are run in an enclosed cable reticulation system.

Covers for enclosed cable reticulation systems

In shared 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: 3; Updated: Dec-21; Applicability: All

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

Security Control: 0195; Revision: 6; Updated: Dec-21; Applicability: TS

In shared facilities, uniquely identifiable SCEC endorsed tamper-evident seals are used to seal all removable covers on TOP SECRET cable reticulation systems.

Security Control: 0194; Revision: 3; Updated: Dec-21; Applicability: TS

In shared facilities, a visible smear of conduit glue is used to seal all plastic conduit joints and TOP SECRET conduits connected by threaded lock nuts.

Labelling conduits

Labels for TOP SECRET conduits should be of sufficient 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: All

Cables from cable trays to wall outlet boxes are run in flexible or plastic conduit.

Cables in party walls

In shared facilities, TOP SECRET cables are not run in party walls; however, an inner wall can be used to run TOP SECRET cables where sufficient space exists for their inspection.

Security Control: 1133; Revision: 3; Updated: Dec-21; Applicability: TS

In shared facilities, TOP SECRET cables are not run in party walls.

Wall penetrations

Penetrating a wall between a TOP SECRET area and a lower classified area requires the integrity of the TOP SECRET area to be maintained. In such scenarios, TOP SECRET cables should be encased in conduit with all gaps between the TOP SECRET conduit and the wall filled with an appropriate sealing compound.

Security Control: 1122; Revision: 2; Updated: Dec-21; Applicability: TS

Where wall penetrations exit a TOP SECRET area into a lower classified area, TOP SECRET cables are encased in conduit with all gaps between the TOP SECRET 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 types of connectors allocated to various systems.

Security Control: 1104; Revision: 4; Updated: Dec-21; Applicability: All

Wall outlet boxes have connectors on opposite sides of the wall outlet box if the cable group contains cables belonging to different systems.

Security Control: 1105; Revision: 3; Updated: Mar-21; Applicability: All

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 to the wrong wall outlet box. In cases where a wall outlet box has a cable group containing cables belonging to different systems, each connector should be individually labelled.

Security Control: 1095; Revision: 5; Updated: Dec-21; Applicability: All

Wall outlet boxes denote the systems, 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 SECRET and TOP SECRET systems from other systems. For example, while SECRET and TOP SECRET wall outlet boxes have designated colours, wall outlet boxes for other systems may be any colour except for those reserved for SECRET and TOP SECRET systems. In addition, wall outlet box colours for other 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: 5; Updated: Dec-21; Applicability: O, P

OFFICIAL and PROTECTED wall outlet boxes are coloured neither salmon pink nor red.

Security Control: 1720; Revision: 0; Updated: Dec-21; Applicability: S

SECRET wall outlet boxes are coloured salmon pink.

Security Control: 1721; Revision: 0; Updated: Dec-21; Applicability: TS

TOP SECRET wall outlet boxes are coloured red.

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: All

Wall outlet box covers are clear plastic.

Fly lead installation

Keeping the lengths of TOP SECRET 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, TOP SECRET fibre-optic fly leads should be treated as cabling infrastructure and run in TOP SECRET conduit or fixed infrastructure such as desk partitioning.

Security Control: 0218; Revision: 6; Updated: Dec-21; Applicability: TS

If TOP SECRET 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 reticulation systems to cabinets can assist in preventing unauthorised modifications and tampering while also providing easy inspection of cables.

Security Control: 1102; Revision: 3; Updated: Dec-21; Applicability: All

Cable reticulation systems leading into cabinets are terminated as close as possible to the cabinet.

Security Control: 1101; Revision: 3; Updated: Dec-21; Applicability: O, P, S, TS

In TOP SECRET areas, cable reticulation systems leading into cabinets in server rooms or communications rooms are terminated as close as possible to the cabinet.

Security Control: 1103; Revision: 3; Updated: Dec-21; Applicability: O, P, S, TS

In TOP SECRET areas, cable reticulation systems leading into cabinets not in server rooms or communications rooms 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: 4; Updated: Dec-21; Applicability: All

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: All

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 rooms

Audio secure rooms are designed to prevent audio conversations from being overheard. The Australian Security Intelligence Organisation should be consulted before any modifications are made to TOP SECRET audio secure rooms.

Security Control: 0198; Revision: 3; Updated: Dec-21; Applicability: TS

When penetrating a TOP SECRET audio secure room, the Australian Security Intelligence Organisation is consulted and all directions provided are complied with.

Power reticulation

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: 3; Updated: Dec-21; Applicability: TS

A power distribution board with a feed from an Uninterruptible Power Supply is used to power all TOP SECRET ICT equipment.

Further information

[Australian cabling standards and regulations](#) can be obtained from the Australian Communications and Media Authority.

Further information on audio secure rooms can be found in the Attorney-General's Department's [Protective Security Policy Framework](#), [Physical security for entity resources](#) policy.

Further information on endorsed seals for various sealing requirements is available in the SCEC's [Security Equipment Evaluated Products List](#).

Emission security

Emission security threat assessments in Australia

Obtaining advice from the Australian Cyber Security Centre (ACSC) on potential adversaries, and appropriate emanation security controls, is vital to protecting SECRET and TOP SECRET systems.

Security Control: 0248; Revision: 6; Updated: Dec-21; Applicability: O, P

System owners deploying OFFICIAL or PROTECTED systems with Radio Frequency transmitters that will be co-located with SECRET or TOP SECRET systems contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the threat assessment.

Security Control: 0247; Revision: 4; Updated: Dec-21; Applicability: S, TS

System owners deploying SECRET or TOP SECRET systems with Radio Frequency 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 threat assessment.

Security Control: 1137; Revision: 3; Updated: Dec-21; Applicability: S, TS

System owners deploying SECRET or TOP SECRET systems in shared facilities contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the threat assessment.

Emission security threat assessments outside Australia

Fixed sites outside Australia, and deployed military platforms, are more vulnerable to emanation security threats. Failing to implement emanation security controls could result in systems or military platforms emanating compromising signals, which if intercepted and analysed, could lead to serious consequences.

Security Control: 0249; Revision: 4; Updated: Dec-21; Applicability: O, P, S, TS

System owners deploying systems or military platforms overseas contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the threat assessment.

Early identification of emanation security controls

It is important to identify emanation security controls for systems early in their project life cycle as costs will be much greater if changes have to be made once a 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.

Electromagnetic interference/electromagnetic compatibility standards

While all ICT equipment may not need certification to emanation security standards, it still needs to meet applicable industry and government standards relating to electromagnetic interference/electromagnetic compatibility.

Security Control: 0250; Revision: 4; Updated: Dec-21; Applicability: All

ICT equipment meets industry and government standards relating to electromagnetic interference/electromagnetic compatibility.