Guidelines for communications infrastructure

**Cable management**

**Applicability**

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

When designing cable management systems, the *Cable labelling and registration* and *Cable patching* sections of these guidelines also apply.

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. Specific requirements for any of these scenarios will be identified as such.

A non-shared government facility is where the entire facility and personnel are cleared to the highest level of information 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.

**Cable sheaths and conduits**

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

**Cable standards**

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

*Security Control: 0181; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must*

Cables are installed in accordance with the relevant Australian Standards, as directed by the Australian Communications and Media Authority (ACMA).
Cable colours

The use of defined cable colours provides an easily recognisable cable management system.

Security Control: 0926; Revision: 5; Updated: Sep-18; Applicability: O, P, S; Priority: Should

The cable colours in the following table are used in non-TOP SECRET areas.

<table>
<thead>
<tr>
<th>System</th>
<th>Cable Colour</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECRET</td>
<td>Pink</td>
</tr>
<tr>
<td>PROTECTED</td>
<td>Blue</td>
</tr>
<tr>
<td>OFFICIAL</td>
<td>Black or grey</td>
</tr>
</tbody>
</table>

Security Control: 0186; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must

The cable colours in the following table are used in TOP SECRET areas.

<table>
<thead>
<tr>
<th>System</th>
<th>Cable Colour</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOP SECRET</td>
<td>Red</td>
</tr>
<tr>
<td>SECRET</td>
<td>Pink</td>
</tr>
<tr>
<td>PROTECTED</td>
<td>Blue</td>
</tr>
<tr>
<td>OFFICIAL</td>
<td>Black or grey</td>
</tr>
</tbody>
</table>

Cable colours for foreign systems in Australian facilities

Different cable colours for foreign systems in Australian facilities helps prevent unintended cross-patching of Australian and foreign systems.

Security Control: 0825; Revision: 1; Updated: Sep-18; Applicability: O, P, S; Priority: Should

Cable colours for foreign systems installed in Australian facilities are not the same colour as those used for Australian systems.

Security Control: 0827; Revision: 1; Updated: Sep-18; Applicability: TS; Priority: Must

Cable colours for foreign systems installed in Australian facilities are not the same colour as those used for Australian systems.

Security Control: 0826; Revision: 1; Updated: Sep-18; Applicability: O, P, S; Priority: Should

Cable colours used for foreign systems are agreed between the host organisation and the foreign system’s owner.

Security Control: 0828; Revision: 1; Updated: Sep-18; Applicability: TS; Priority: Must

Cable colours used for foreign systems are agreed between the host organisation and the foreign system’s owner.

Cable colour non-conformance

In certain circumstances it may not be possible to use the correct cable colours. Under these circumstances organisations are to band cables with the appropriate colour. The banding of cables is to comply with the inspection points for the cables. The size of the cable bands should be easily visible from the inspection point. For large bundles on cable reticulation systems, band and label the entire bundle. It is important bands are robust and 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: 1215; Revision: 1; Updated: Sep-18; Applicability: O, P, S; Priority: Must**

In non-TOP SECRET areas, cables with non-conformant cable colouring are banded with the appropriate colour at inspection points.

**Security Control: 1216; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must**

In TOP SECRET areas, cables with non-conformant cable colouring are both banded with the appropriate colour and labelled at inspection points.

**Inspecting cables**

Regular inspection of cable installations is necessary to detect illicit tampering or degradation.

**Security Control: 1112; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should**

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; Priority: Should**

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; Priority: Should**

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, Priority: Should**

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; Priority: Must**

In TOP SECRET areas of shared non-government facilities, cables are fully inspectable for their entire length.

**Cable groupings**

Grouping cables provides a method of sharing conduits and cable reticulation systems.

**Security Control: 0187; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must**

The approved group combinations for cables in the following table are used.

<table>
<thead>
<tr>
<th>Group</th>
<th>Approved Combination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OFFICIAL</td>
</tr>
<tr>
<td></td>
<td>PROTECTED</td>
</tr>
<tr>
<td>2</td>
<td>SECRET</td>
</tr>
<tr>
<td>3</td>
<td>TOP SECRET</td>
</tr>
</tbody>
</table>

**Use of fibre-optic cables**

Fibre-optic cables do not produce, and are not influenced by, electromagnetic emanations. Therefore, they offer the highest degree of protection from electromagnetic emanation effects. Fibre-optic cables are also more difficult to tap than copper cables and many more fibres can be run per cable diameter than wired cables reducing cable infrastructure costs.
In non-shared government facilities, fibre-optic cables are used for network infrastructure instead of copper cables.

In shared government facilities, fibre-optic cables are used for network infrastructure instead of copper cables.

In non-TOP SECRET areas of shared non-government facilities, fibre-optic cables are used for network infrastructure instead of copper cables.

Fibre-optic cables sharing a common conduit

Fibre-optic cables of various cable groups can share a common conduit to reduce costs.

With fibre-optic cables, the fibres in the sheath only carry a single group.

If a fibre-optic cable contains subunits, each subunit only carries a single group; however, each subunit in the cable can carry a different group.

Laying cables in a neat and controlled manner that allows for inspection reduces the need for individual cable trays.
In non-shared government facilities, approved cable groups sharing a common reticulation system have a dividing partition or a visible gap between the differing cable groups.

In shared government facilities, approved cable groups sharing a common reticulation system have a dividing partition or a visible gap between the individual cable groups.

In non-TOP SECRET areas of shared non-government facilities, approved cable groups sharing a common reticulation system have a dividing partition or a visible gap between the differing cable groups.

In TOP SECRET areas of shared non-government facilities, approved cable groups sharing a common reticulation system have a dividing partition or a visible gap between the differing cable groups.

Enclosed cable reticulation systems

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

In non-TOP SECRET areas of shared non-government facilities, cables are run in an enclosed cable reticulation system.

In TOP SECRET areas of 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 reticulation systems are a convenient method of maintaining inspection and control requirements. Having clear covers face inwards increases their inspectability.

In non-TOP SECRET areas of shared non-government facilities, conduits or the front covers of ducts, cable trays in floors and ceilings, and associated fittings are clear plastic.

In TOP SECRET areas of 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 are used to provide evidence of any tampering or illicit access to cable reticulation systems while conduits are sealed with a visible smear of conduit glue to prevent access.

In shared non-government facilities, uniquely identifiable SCEC endorsed tamper-evident seals are used to seal all removable covers on reticulation systems, including box section front covers, conduit inspection boxes, outlet and junction boxes, and T-pieces.

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.
Connecting cable reticulation systems to cabinets

Strictly controlling the routing from cable management systems to cabinets prevents unauthorised modifications and tampering and provides easy inspection of cables.

**Security Control: 1102; Revision: 1; Updated: Sep-18; Applicability: O, P, S; Priority: Should**
In non-TOP SECRET areas, reticulation systems leading into cabinets are terminated as close as possible to the cabinet.

**Security Control: 1101; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should**
In TOP SECRET areas, 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: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must**
In TOP SECRET areas, 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 prevents accidental or deliberate cross-patching and makes visual inspection of cables and patching easier.

**Security Control: 1098; Revision: 1; Updated: Sep-18; Applicability: O, P, S; Priority: Should**
In non-TOP SECRET areas, cables are terminated in individual cabinets, or for small systems, one cabinet with a division plate to delineate classifications.

**Security Control: 1099; Revision: 1; Updated: Sep-18; Applicability: O, P, S; Priority: Must**
In TOP SECRET areas, cables are terminated in individual cabinets, or for small systems, one cabinet with a division plate to delineate classifications.

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

Cabinet separation

Having a definite gap between cabinets allows for ease of inspection for any illicit cables or cross-patching.

**Security Control: 1116; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should**
In non-shared government facilities, there is a visible gap between TOP SECRET cabinets and cabinets of lower classifications.

**Security Control: 1124; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should**
In shared government facilities, there is a visible gap between TOP SECRET cabinets and cabinets of lower classifications.

**Security Control: 1136; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must**
In shared non-government facilities, there is a visible gap between TOP SECRET cabinets and cabinets of lower classifications.

Cables in walls

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

**Security Control: 1115; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should**
In non-shared government facilities, cables from cable trays to wall outlets are run in flexible or plastic conduit.

**Security Control: 1121; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should**
In shared government facilities, cables from cable trays to wall outlets are run in flexible or plastic conduit.
In shared non-government facilities, cables from cable trays to wall outlets are run in flexible or plastic conduit.

**Cables in party walls**

In shared non-government facilities, cables are not allowed in a party wall. A party wall is a 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.

**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 are encased in conduit with no gaps in the wall around the conduit.

**Wall outlet terminations**

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

**Wall outlet colours**

The colouring of wall outlets makes it easy to identify TOP SECRET infrastructure.

**Wall outlet covers**

Transparent covers on wall outlets allow for inspection of cable cross-patching and tampering.
In TOP SECRET areas, faceplates on wall outlets are clear plastic.

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.

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.

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.

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


Cable labelling and registration

Applicability

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

Conduit label specifications

Conduit labels should be a specific size and colour to allow for easy identification of secure conduits carrying cables.

Labels for TOP SECRET conduits are a minimum size of 2.5 cm x 1 cm, attached at 5 m intervals and marked as ‘TS RUN’.

Conduit labels in areas where uncleared personnel could frequently visit have red text on a clear background.

Conduit labels in areas that are not clearly observable have red text on a white background.
Installing conduit labelling

Conduit labelling in public or visitor areas could draw undue attention and disclose capabilities.

Security Control: 0204; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Conduit labels installed in public or visitor areas do not draw undue attention from people who do not have a need-to-know of the existence of such cables.

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 outlet.

Security Control: 1095; Revision: 1; Updated: Sep-18; Applicability: O, P, S; Priority: Should
Wall outlet boxes denote the classification, cable number and outlet number.

Security Control: 0205; Revision: 2; Updated: Sep-18; Applicability: TS; Priority: Must
Wall outlet boxes denote the classification, cable number and outlet number.

Standard Operating Procedures

Documenting labelling conventions in Standard Operating Procedures (SOPs) makes cable and fault finding easier.

Security Control: 0206; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Site conventions for labelling and registration of cables are documented in SOPs.

Labelling cables

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

Security Control: 1096; Revision: 1; Updated: Sep-18; Applicability: O, P, S; Priority: Should
Cables are labelled at each end with sufficient source and destination details to enable the physical identification and inspection of the cable.

Security Control: 0207; Revision: 2; Updated: Sep-18; Applicability: TS; Priority: Must
Cables are labelled at each end with sufficient source and destination details to enable the physical identification and inspection of the cable.

Cable register

Cable registers allow installers and inspectors to trace cables for cable inspections and malicious or accidental damage. Cable registers track all cable management changes throughout the life of the system.

Security Control: 0208; Revision: 1; Updated: Sep-18; Applicability: O, P, S; Priority: Should
A cable register is maintained with the following information:

- cable identification number
- classification
- source
- destination
- site/floor plan diagram
- seal numbers (if applicable).
Security Control: 0210; Revision: 2; Updated: Sep-18; Applicability: TS; Priority: Must
A cable register is maintained with the following information:

- cable identification number
- classification
- source
- destination
- site/floor plan diagram
- seal numbers (if applicable).

Cable inspections

Cable inspections, at predefined periods, are a method of checking the cable management system with the cable register.

Security Control: 0211; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Cables are inspected for inconsistencies with the cable register in accordance with the frequency defined in a system’s System Security Plan (SSP).

Cable patching

Applicability

The security controls in this section apply to new cable installations or upgrades. Organisations do not need to retrofit existing cable 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.

Terminations to patch panels

Connecting a system to another system of a lower classification will result in a data spill, possibly resulting in inadvertent or deliberate access by non-cleared personnel, or the lower system not meeting the appropriate requirements to secure the information from unauthorised access or tampering.

Security Control: 0213; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Only approved cable groups terminate on a patch panel.

Patch cable and fly lead connectors

Ensuring that cables are equipped with connectors of a different configuration to all other cables prevents inadvertent connection of different systems.

Security Control: 1093; Revision: 2; Updated: Sep-18; Applicability: O, P, S; Priority: Should
In areas containing cables for systems of different classifications, connectors for each system are different from those of other systems; unless the higher classified patch cables cannot bridge the distance between the higher classified patch panel and any patch panel of a lower classification.

Security Control: 0214; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
In areas containing cables for TOP SECRET systems and systems of lower classifications, the connectors for TOP SECRET systems are different from those of other systems.
In areas containing cables for systems of different classifications, the selection of connector types is documented.

In areas containing cables for TOP SECRET systems and systems of lower classifications, the selection of connector types is documented.

Physical separation of patch panels

Appropriate physical separation between a TOP SECRET system and a system of a lower classification reduces or eliminates the chances of cross-patching between systems and reduces or eliminates the possibility of unauthorised personnel gaining access to TOP SECRET systems.

TOP SECRET and non-TOP SECRET patch panels are physically separated by installing them in separate cabinets.

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.

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 infrastructure and run in conduit or fixed infrastructure such as desk partitioning.

If fibre-optic fly leads exceeding five meters in length are used to connect wall outlets to ICT equipment, they are run in a protective and easily inspected pathway and clearly labelled at the ICT equipment end with the wall outlet’s designator.

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 information.

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.
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; Priority: Must**
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; Priority: Must**
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 SOPs 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; Priority: Should**
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; Priority: Must**
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; Priority: Should**
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; Priority: Must**
ICT equipment in TOP SECRET areas meets industry and government standards relating to electromagnetic interference/electromagnetic compatibility.

**Further information**

Further information on cables and separation standards, as well as the potential dangers of operating RF transmitters near systems is documented in Australian Communications Security Instruction (ACSI) 61 D.

Further information on conducting an emanation security threat assessment is documented in ACSI 71 D.