Australian Communications-Electronic Security Instruction 33 (ACSI 33)

Point of Contact: Customer Services Team

Phone: 02 6265 0197 Email: assist@dsd.gov.au

HANDBOOK 5

EMANATIONS AND CABLING SECURITY

Version 1.0

General

501. The term TEMPEST is widely associated with emanation security. TEMPEST is the study of electro-magnetic signals bearing compromising information emanating from electronic processing equipment and cabling. All IT systems, office and communication equipment and information-bearing cabling, used for the processing and/or communication of sensitive information, produce unintended electro-magnetic emanations that are related to the information being processed or communicated. Analysis of these emanations may allow the recovery of the original information, which can then be exploited. The availability of "high tech" equipment and information to the general populous has increased the awareness of TEMPEST exploitation.

TEMPEST Threat

502. DSD is the National Authority for the assessment of TEMPEST threat. Any agency with TEMPEST concerns should contact DSD for advice.

503. A TEMPEST risk assessment should be factored into the more general risk assessment process, as detailed in **Handbook 3 - Risk Management**. In assessing the TEMPEST risk current and future TEMPEST threats should be identified. It is important to place TEMPEST into the context of the overall threats to an organisation. It is essential to assess carefully the threat to the information processed by the installation to ensure that the protective measures are both justified and adequate. By considering future requirements, costs of system upgrades and expansion may be reduced. The value of sound judgement and common sense in the risk assessment process cannot be over-

stated. In most cases, agencies running non-national security data could consider assigning a lower priority to tempest countermeasures. Agencies should consider the TEMPEST threat in the context of their physical security environment.

TEMPEST Countermeasure

504. Implementing TEMPEST countermeasures can significantly increase costs of equipment, cable infrastructures and administrative overhead. TEMPEST countermeasures should only be implemented when identified in the TEMPEST risk assessment. DSD should be consulted on the appropriateness of the measures. Some examples of TEMPEST countermeasures are listed below.

a. Enclosing the IT or Communication system within a screened room or building.

b. Use TEMPEST rated or tested equipment

c. Use of fibre optic cabling will eliminate cable TEMPEST conduction and radiation.

d. Filters (eg power, telephone) will reduce TEMPEST conduction.

e. Separation of equipment and cabling of differently classified systems.

f. Increase and manage the controlled space to prevent unauthorised access near classified systems.

g. National Security Installations should be planned in accordance with the guidance contained in current endorsed installation standards.

h. Prevent equipment tampering during transit or repair.

TEMPEST Equipment

505. Certified TEMPEST equipment can be expensive. Certified TEMPEST equipment is not normally warranted for Non-National Security classified systems. Equipment manufactured to EMI/EMC (AS3548 for Australia) standards is recommended. If Certified TEMPEST equipment is being considered, then DSD advice should be sought.

Cabling Security

506. The TEMPEST Risk assessment should consider the impact on changes in threat, upgrading to a higher classification level and future expansion of the cabling infrastructure. Cabling and access points should be provided with equivalent protection mechanisms as is provided to agency classified data storage areas.

507. Some security objectives for cabling are:

a. To implement effective configuration control. Separation of classified and unclassified cabling.

b. To physically protect cabling, patch panels, IDF and PABX cabling from unauthorised access (eg line tapping, malicious damage).

c. To enable cables to be readily inspected for tampering and correctness.

d. To reduce the risk of classified cabling being inadvertently or deliberately patched into unclassified networks.

e. Prevent TEMPEST emanations from cabling if identified by the risk assessment (screening cables, converting to fibre cable).

f. Prevent / detect unauthorised connection of equipment into the cabling system.