10.7. Emanation Security Threat Assessments

Objective

10.7.1. In order to minimise compromising emanations or the opportunity for a technical attack, a threat assessment is used to determine appropriate countermeasures.

Context

Scope

10.7.2. This section relates to emanation security threat assessment advice and identification of appropriate countermeasures to minimise the loss of classified information through compromising emanations or a technical attack.

10.7.3. This section is applicable to:

- agencies located outside New Zealand;
- secure facilities within New Zealand; and
- mobile platforms and deployable assets that process classified information.

References

10.7.4. Information on conducting an emanation security threat assessment and additional information on cabling and separation standards, as well as the potential dangers of operating RF transmitters in proximity to classified systems, is documented in:

Reference	Title	Publisher	Source
NZCSS 400	**Installation Engineering**	GCSB	CONFIDENTIAL document available on application to authorised personnel
NZCSI 403B	**TEMPEST Threat and Countermeasures Assessment**	GCSB	CONFIDENTIAL document available on application to authorised personnel
NZCSI 420	**Laboratory Tempest Test Standard for Equipment in Controlled Environments**	GCSB	CONFIDENTIAL document available on application to authorised personnel

PSR references

10.7.5. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	Home | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Physical security (PHYSEC) | Protective Security Requirements

Rationale & Controls

Emanation security threat assessments within New Zealand

10.7.6.R.01. **Rationale**

Obtaining the current threat advice from GCSB on potential adversaries and threats and applying the appropriate countermeasures is vital in maintaining the confidentiality of classified systems from an emanation security attack.

10.7.6.R.02. **Rationale**

Failing to implement recommended countermeasures against an emanation security attack can lead to compromise. Having a good cable infrastructure and installation methodology will provide a strong backbone that will not need updating if the threat increases. Infrastructure is very expensive and time consuming to retro-fit.

10.7.6.C.01. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:2454]

Agencies designing and installing systems with RF transmitters within or co-located with their facility MUST:

- contact GCSB for guidance on conducting an emanation security threat assessment; and
- install cabling and equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

10.7.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2455]

Agencies designing and installing systems with RF transmitters that co-locate with systems of a classification CONFIDENTIAL and above MUST:

- contact GCSB for guidance on conducting an emanation security threat assessment; and
- install cabling and equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

Emanation security threat assessment outside New Zealand

10.7.7.R.01. **Rationale**

Fixed sites and deployed military platforms are more vulnerable to emanation security attack and require a current threat assessment and countermeasure implementation. Failing to implement recommended countermeasures 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.

10.7.7.C.01. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:2458]

Agencies deploying systems overseas in temporary, mobile or fixed locations MUST:

- contact GCSB for assistance with conducting an emanation security threat assessment; and
- install cabling and equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

10.7.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2459]

Agencies deploying systems overseas SHOULD:

- contact GCSB for assistance with conducting an emanation security threat advice; and
- install cabling and equipment in accordance with this document plus any specific installation criteria derived from the emanation security threat assessment.

Early identification of emanation security issues

10.7.8.R.01. **Rationale**

The identification of emanation security controls that need to be implemented for a system at an early stage in the project lifecycle. This can significantly affect project costs. Costs are invariably greater where changes are necessary once the system had been designed or has been implemented.

10.7.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2463]

Agencies SHOULD conduct an emanation security threat assessment as early as possible in project lifecycles.

IT equipment in SECURE areas

10.7.9.R.01. **Rationale**

All equipment must conform to applicable industry and government standards, including NZCSI 420; Laboratory Tempest Test Standard for Equipment in Controlled Environments. Not all equipment within a secure facility in New Zealand requires testing against TEMPEST standards.

10.7.9.C.01. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must** [CID:2465]

Agencies MUST ensure that IT equipment within secure areas meet industry and government standards relating to electromagnetic interference/electromagnetic compatibility.