



TEMPEST Introduction

Introduction

The following is intended as an introduction to TEMPEST.

What is TEMPEST?

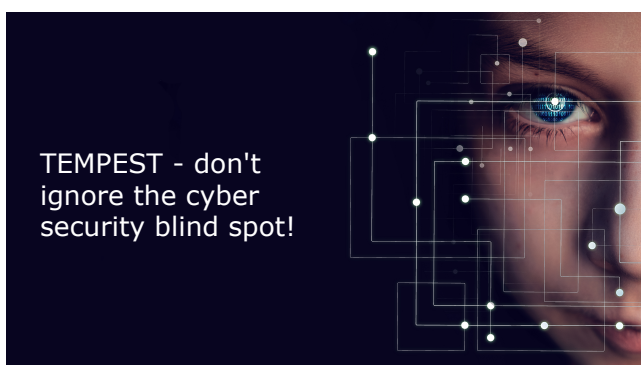
All electrical and electronic equipment produces electromagnetic radiation (electrical emanations). The electromagnetic signals propagate through space (radiated emissions) and along electrically conductive pathways (conducted emissions).

If these emissions are intercepted and analysed they could reveal that the signals contain information rather than merely 'noise' and thus the protectively marked data could be revealed. A receiving device can intercept these signals without being detected even when located some distance away, access to the original equipment is not required.

Electromagnetic testing for commercial items, for instance as part of the CE compliance procedure, examines both the power of the emissions (signal strength) to ensure that it will not adversely affect other products in the locality and the tested items susceptibility to electromagnetic radiation generated from other sources to ensure it will not itself be adversely affected.

TEMPEST is concerned with only the emitted radiation (both radiated and conducted) and whether the signal is 'information bearing'.

TEMPEST is defined as the study of the unintentional emission of protectively marked data from an equipment or system.



The silent threat of covert eavesdropping is still very real.

Commonplace IT electronic noise can be information bearing and encryption is redundant if source data can be stolen and analysed.

Data integrity is vital, and any compromise or breach can lead to financial, political and, or life-threatening consequences.

A brief history of TEMPEST

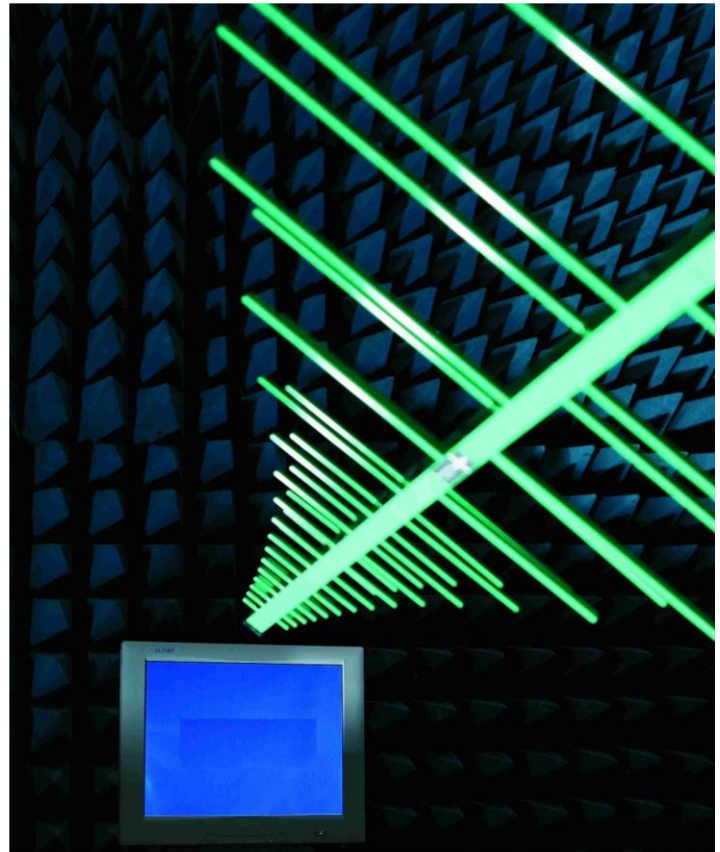


The ability to collect electromagnetic radiation from signal processing equipment has been known about since the 1940's.

The study of emissions, the effort to secure electronic equipment and the ability to intercept and interpret those signals from other sources were brought under the codename TEMPEST.

Contrary to some beliefs TEMPEST is not an acronym and does not have an actual meaning.

Until relatively recently the codename TEMPEST and even the existence of the study and countermeasures was highly classified. All details of testing, signals, limits, test results and countermeasures remain protectively marked to a very high level.



TEMPEST Standards

The following standards are used for the specification of TEMPEST equipment.

<i>Descriptive</i>	Full	Intermediate	Tactical
SDIP-27 NATO Standard	Level A	Level B	Level C
Previous NATO Laboratory test Standards	AMSG-720B	AMSG-788A	AMSG-784
NATO Zoning Standards	ZONE 0	ZONE 1	ZONE 2
USA NSTISSAM /1-92 Standards	LEVEL I	LEVEL II	LEVEL III



TEMPEST Standards continued

In addition to the previous table for TEMPEST equipment standards, the following standards are pertinent when considering installations:

- **SDIP-27**, which has replaced the AMMSG-720B / AMMSG-788A / AMMSG-784
(NATO TEMPEST requirements and Evaluation procedures)
- **SDIP-28**, which has replaced AMMSG-799 (NATO Zoning Procedures)
- **SDIP-29**, which has replaced AMMSG 719 (Facility Design Criteria and Installation of Electrical Equipment for Processing Classified Information)
- **SDIP-30** Installation of electronic equipment for processing of classified data

TEMPEST equipment and installation standards detail

- NATO SDIP-27 Level A (formerly AMMSG 720B) and USA NSTISSAM Level I
This is the strictest standard for devices that will be operated in NATO Zone 0 environments. TEMPEST items to this standard offer the highest level of protection.
- NATO SDIP-27 Level B (formerly AMMSG 788A) and USA NSTISSAM Level II
"Laboratory Test Standard for Protected Facility Equipment"
This is a standard for devices that are operated in NATO Zone 1 environments.
- NATO SDIP-27 Level C (formerly AMMSG 784) and USA NSTISSAM Level III
"Laboratory Test Standard for Tactical Mobile Equipment/Systems"
A standard for devices operated in NATO Zone 2 environments and of particular reference to mobile and installed platforms.
- NATO SDIP-29 (formerly AMMSG 719G)
"Installation of Electrical Equipment for the Processing of Classified Information"
This standard defines installation requirements, for example in respect to grounding and cable distances.
- NATO SDIP-28 (formerly AMMSG 799B) "NATO Zoning Procedures"
Defines a procedure according to which individual areas within a security perimeter can be classified into Zones which then determines the standard required for installed equipment.

Glossary Of Acronyms

- **TEMPEST** – a codeword, not an acronym!
- **SDIP** - SECAN Doctrine and Information Publication
- **SECAN** - SECurity and Evaluation Agency
- **AMMSG** – Allied Military Security Guide
- **NSTISSAM** - National Security Telecommunications and Information Systems Security Advisory Memorandum

About SSIA

- Made up of three distinct brands covering North America and the UK, Emcon & SST brands unite together to achieve the same goal...To be the leading global supplier of highly reliable, engineered TEMPEST, Secure and integrated solutions. Together we offer local expertise with global capabilities.
- We have three dedicated secure design and manufacturing facilities in Canada, the US and the UK. We maintain a NCSC accredited test facility in the UK. NCSC is the UK National Technical Authority for Information Assurance.
- SSIA acts as a TEMPEST authority and subject matter expert for design and installation as part of larger programmes.
- We keep a close relationship with our key OEM partners to ensure we keep up with the ever-increasing speeds of product roadmap cycles.
- SSIA is part of the Spectrum Control group - a global leader in high-performance RF and microwave signal processing and conditioning, and electromagnetic interference protection.
- We offer a robust portfolio of TEMPEST products including desktops, mobile and rugged, printers, networking devices, VoIP and custom fly-away kits.



National Cyber Security Centre

