

## CHAPTER 28

### TEMPEST PROTECTION SYSTEMS

---

#### 28-1. General TEMPEST protection systems

This chapter addresses systems constructed to prevent adversaries acquiring compromising information from facilities containing classified information. Facilities house equipment that are sources of electromagnetic (EM) waves and stray currents/voltages with characteristics which are related to the information content of the signals being processed. If these unintentional emissions are intercepted and studied, the analyst can reconstruct the original data and can obtain access to classified national security information. TEMPEST (military code-name) protection systems will, preclude the presence of analyzable signals in uncontrolled areas by controlling EM energy and, thus, provide communication security.

*a. Scope.* TEMPEST is a U. S. Department of Defense program to develop methods of preventing the compromise of government and military information. This is accomplished by reducing or eliminating unintended electric or EM radiation emanations from electronic equipment. The present approach focuses on "threat-based systems approach" in an effort to reduce the high cost of TEMPEST efforts. Emission Security (EMSEC) is another term that has found favor and covers all emanations with potential to compromise national security information and the measures employed to prevent unauthorized disclosure.

*b. Objectives.* The TEMPEST problem is nearly the inverse of the High-Altitude Electromagnetic Pulse (HEMP) event. TEMPEST is the unclassified name for the studies and investigation of compromising emanations. Equipment within the facility can be the source of EM waves and stray currents/voltages with characteristics that are related to the information content of signals being processed. Thus, HEMP and TEMPEST protective measures must each control EM energy, the former protecting system equipment from externally generated signals and the latter containing emissions from internal sources. The functional similarities imply that a common treatment can be employed for the two purposes.

#### 28-2. Sources

Compromising emanations may be generated by any electrical information processing equipment. Some of them are microchips, computers, monitors, printers, and electronic typewriters. These emanations can be propagated through space, over telephone lines, power lines, water pipes, grounding wires, ducts, drains, and conduit.

#### 28-3. Acquisition

Using specialized antennae, low noise pre-amps, filters, and top end receivers with computer interfaces it is possible to access sensitive information for immediate interpretation or analysis later. Unclassified estimates place interception ranges at 1 km.

#### 28-4. Protection

To mitigate or eliminate compromises in security, several techniques are used.

*a. Evaluation.* TEMPEST measures shall be weighted based on the sensitivity of information, the amount of classified information, and the probability of facility becoming an intercept target.

*b. Personnel control.* Equipment must be kept physically secure by providing physical controls to prevent, delay, and detect unauthorized access to the central computer facility, internal controlled areas, peripheral devices, remote terminals, and storage media. In many cases, the physical controls consist of determining what personnel may enter or leave a given site, and what equipment must be kept under controlled circumstances. The current emphasis in military systems is on dedicated computer systems.

*c. Compartmentalism.* TEMPEST protection requires that information under one classification and compartment be isolated from other classifications and compartments. The separation requirements are based on "Equipment Radiation Transmission Zone (ERTZ)." Emanations are allowed within the ERTZ as determined by engineering estimates, ambient noise levels (masking), facility construction, and distance from source.

*d. Physical controls.* It is a requirement that electronic equipment used for classified processing be shielded or designed to reduce or eliminate transient emanations.

(1) One method is to shield the area in which the information is processed so as to contain EM emanations or to specify control of certain distances or zones beyond which the emanations cannot be detected. In many cases, facilities are required to be kept within complete metal enclosures to prevent EM leakages, and vacuum seals to prevent sonic leakages. High noise environments are sometimes artificially generated to make the detection of signals very difficult. Shielding can also be applied to equipment cabinets and chassis via radio frequency interference (RFI) seals and honeycomb filter doors.

(2) Unless the wiring (telephone lines, electrical wiring, network cables, etc.), is shielded the other shielding methods discussed will not stop emanations from leaking to the outside world. All conductors must be isolated at the point of egression, including drains, pipes, ducts, cable trays, and conduits.

(3) Separating classified and unclassified equipment transmission paths can eliminate this form of cross cable leakage. Power lines for classified equipment must be isolated.

(4) EM signal strength can be minimized by filtering signals on the electrical leads. This is accomplished by using ferrites and optically coupled filters. Power lines for classified equipment must be filtered.

(5) Station earth ground point must not be shared by any other facility. Classified equipment must be properly grounded.