

INDUSTRIAL TEMPEST PROGRAM

All electronic equipment emits extraneous electromagnetic energy. When this energy causes operational problems in other equipment, a condition of electromagnetic interference (EMI) is said to exist. In the case of equipment that processes information, it is possible to extract extraneous energy related to the data being processed. If that data is classified, a security compromise is a distinct possibility. This problem is referred to by the unclassified short name (not an acronym) "TEMPEST". Although many of the basic engineering techniques used to prevent a TEMPEST problem are similar to those used to avoid EMI, the evaluation techniques and criteria for acceptability are substantially different. A piece of equipment can be electromagnetically compatible with surrounding systems (and, in fact, fully compliant with MIL-STD-461A, the military standard for electromagnetic interference), and still be a TEMPEST hazard. The converse is also true. That is, equipment can fully comply with TEMPEST requirements while, at the same time, emit high levels of non-information-bearing electromagnetic energy. The engineer who deals with both EMI and TEMPEST must be able to wear two very different hats.

Whenever a government contract requires equipment to comply with a TEMPEST specification, there is a reasonable chance that it will be processing classified information. To provide an unauthorized interested observer with information regarding the TEMPEST characteristics of that equipment, and how such characteristics are evaluated, would be tantamount to leaving the combination to your security file written on your office blackboard. Therefore, there has been, and will continue to be, a very real requirement to safeguard technical information regarding TEMPEST test procedures, analysis techniques, acceptability criteria, suppression methods, and especially the emission characteristics of any equipment which the government might use to process classified information.

Because of the classification of the information, the government TEMPEST community has not divulged much more than the simple definition of "TEMPEST" except under strict conditions of need-to-know. This lack of technical communication existing between industry and the government resulted in a situation which had two basic problems: First, contractors were not knowledgeable about TEMPEST, its implications, or its solutions. Therefore, any RFQ for equipment which included TEMPEST requirements could expect a cost response with a large built-in contingency factor to cover the unknown TEMPEST quantity. Second, for TEMPEST engineering to keep pace with the state-of-the-art in the important areas of signal detection and analysis, detection system development, and communication system design, the experts in these fields needed to be aware of the TEMPEST problem. Much of the expertise resided, of course, in industry, the very community which was being "kept in the dark".

To help alleviate these problems, The National Security Agency, acting for the government, instituted the "Industrial TEMPEST Program." This has done much to improve the situation by providing a vehicle by which technical TEMPEST information can flow between contractors and government, and between contractors themselves. This is not to say that NSA has relaxed its controls over such information. If anything, they are more closely defined. For example, articles dealing with TEMPEST, such as this one, must be submitted to the National Security Agency for classification review prior to publication. However, within the context of those controls, new channels of communica-

tion are now available for those companies who become voluntary participants in the Industrial TEMPEST Program.

The Industrial TEMPEST Program is not intended to provide an alternate means of obtaining classified information when a means already exists. For example, if classified TEMPEST documents are required in conjunction with the contract or RFQ, the contractor must obtain them from the contracting officer. The Industrial TEMPEST Program is intended to provide a means of obtaining classified TEMPEST information when no contractual requirement exists.

The principal objective of the Industrial TEMPEST Program is to encourage the voluntary development, by industry, of information-processing equipment which complies with the TEMPEST specifications. In the past, the greatest single stumbling block to many companies who needed to learn about TEMPEST, or who had something to contribute to the TEMPEST state-of-the-art, was the fact that without an on-going government contract whose DD-254 (the DoD Contract Security Classification Specification) specifically provided for the possession of TEMPEST documents, such a company was definitely "on the outside looking in," from the standpoint of the TEMPEST community. Now, however, if a company can satisfy various requirements for facility security clearance and classified document storage capability, and can establish to a reasonable degree that it is in the government's interest that the company participate in the Industrial TEMPEST Program, the National Security Agency will assume the responsibilities that the Industrial Security Manual assigns to a contracting officer, and will issue a DD-254 security form. This means that such a company, even though it has no active contracts involving TEMPEST, can receive necessary classified TEMPEST documents. This is of significant benefit to contractors in that it permits them to establish TEMPEST capabilities, both in manpower and capital equipment.

Another significant benefit to participants in the Industrial TEMPEST Program is that it provides for crossfertilization between participants. For example, if Company A manufactures a printer which meets TEMPEST requirements, and if Company B has a need for such a printer, Company B may obtain a copy of the classified TEMPEST Test Report for the printer, *provided* that both companies are participants in the Program, and that Company A provides written permission for Company B to obtain a copy of its Report. Such information exchange within industry will do much to ensure that the government is offered the best available TEMPEST equipment and systems.

Finally, to become a voluntary participant in the Industrial TEMPEST Program, interested companies need only express their interest by writing to

Director, National Security Agency
Fort George G. Meade, Maryland 20755
Attention: S643

NSA will then provide additional information about the Industrial TEMPEST Program.

The above article was written by Daniel J. Norton, Manager, TEMPEST Engineering Section, Sanders Associates, Nashua, N.H. This is a repeat of the original article which appeared in ITEM '77.