WHAT IS TEMPEST?

Because the phenomenon of compromising enations (CEM) is formally explained using electromagnetic field theory, many personnel believe the compromising emanations problem is too complex to understand. While it is not necessary, nor do we expect everyone to have a detailed technical knowledge of TEMPEST, all personnel in the Intelligence Community (IC) should have a basic understanding to appreciate the problem. Further, there is a need to understand what can and cannot be done about TEMPEST.

"TEMPEST is an unclassified short name referring to the study and investigations of compromising emanations."

"Compromising Emanations are unintentional data-related or intelligence-bearing signals which, if intercepted and analyzed, disclose the National security related information transmitted, received, handled or otherwise processed by information-processing equipment." These are the accepted definitions found in National publications concerning compromising emanations, but these definitions do little in helping us to understand the problem.

Let us examine what a compromising emanation is. A compromising emanation is electromagnetic energy unintentionally emitted from equipment that is processing National security related information and that has some characteristic that makes it possible to intercept, analyze, and recover the information. For those of you that do not have a technical background, we include an explanation that may help you to understand what we mean by "unintentional emanation."

You are all familiar with commercial television, radio and cellular telephones where signals are transmitted from one point and received at another by equipment designed for the purpose. In the process of generating these desired signals, there are also many signals produced that are not desired. Normally, these undesired signals are not of any concern and are ignored unless they interfere with the normal operations of other equipment. It is these unintentional emanations (signals) that we are concerned with when they emanate from equipment that is handling National security related information.

For example, it is possible to record and analyze unintentional emanations from electrically-powered equipment and recover, for practical purposes, 100 percent of processed National security related traffic.

The source of compromising emanations is as simple as the arcing of relay contacts to very

complex electronics. All electronic devices have components which emit unintentional emanations. The characteristics of the compromising signal are very complex. So, too, are the tasks of recovering, recording, and analyzing to obtain the National security related information. However, the principle of interception and the possibility of compromise remain the same.

Let us now examine how compromising emanations can occur. Any electrical device, whether an ordinary laptop computer, or a multimillion-dollar data processing center, emits interceptable signals. Depending on the type of equipment and its environment, compromising emanations can be radiated through space as radio waves or conducted on telephone lines, water pipes, or any other conductor leaving the area. The type of signal and the environment determine the type of equipment used to intercept, record, and analyze the signal. The types of compromising emanations that might appear at an intercept point are electromagnetic fields radiated directly by elements processing equipment and associated conductors or text-related signals coupled to signal or power lines through common circuit elements such as grounds, power supplies, or inductive and capacitive coupling to the lines.

A Compromising emanations can occur as:

1) Electromagnetic fields set free by elements of plaintext-processing equipment.

2) Text-related signals coupled to signal or power lines through common circuit elements such as grounds and power supplies or through inductive and capacitive coupling.

3) Amplitude and phase modulation in power lines resulting from load changes. These load changes come as a result of functions related to processing information signals.

4) Sound-wave propagation from mechanical or electromechanical processing devices.

B The immediate causes of the problem signals, as described, are current and voltage changes. Some of the generators of these changes and the major violators are:

1) Commercial input devices. Many types of equipment in use today operate with high-current (20 milliamps, 60 milliamps) and high-voltage (60 volts, 130 volts). The high-intensity fields produced by these equipments are the most dangerous source of compromising emanations.

2) Solid-state devices. The extremely fast-switching action involved in transistor and diode operations produces the sharp-rising pulses that produce undesirable emanations.

3) Vacuum tubes (although rarely in use today). Oscillations generated between tube elements and within the functioning circuits can be modulated by intelligence processing circuits and become information carriers.

4) Zener diodes (although rarely in use today). These are devices used in circuits for equipment operations and are potential “noise” sources. Like vacuum tubes, the signals (noise) need not be related to the plaintext processing to become compromise sources. They can also be modulated by intelligence-processing circuits and become information carriers.

5) Any COMSEC component which performs a function similar to one of those

described above is a possible source. Card readers and facsimile equipment involve some phase of operation capable of generating compromising signals.

C There are other problem areas which might be thought of as sources of compromising emanations. These involve coupling from RED areas (secure) to BLACK areas (unsecure). Some examples are:

1) Printed Circuit Boards and Encapsulated Modules. Since components in these devices are in extremely close relationship and at times functions as parts of different circuits, they can act as coupling elements.

2) Grounds. This type of coupling is perhaps the most difficult to deal with. Coupling through grounds can take place not only directly but also through ground loops; that is, currents circulating around and between physically separated grounds.

3) Equipment Meters and Indicators. These units must often display functions in both RED and BLACK circuits. Since they serve to connect the two areas, these instruments can be coupling devices.

4) Telephones. These instruments can be particularly dangerous as conductors of compromising signals because their presence is often accepted as something apart from the whole information-processing operation. However, the two sensitive elements in each handset and the equally responsive ringing element in the instrument case can be activated by surrounding signals. If this happens, signals are carried a great distance over telephone lines where satisfactory physical protection is not possible.

Many of the sources of emanations which have been mentioned will continue to emanate in spite of the efforts by design engineers. They need now, however, be emendators of compromising signals. Ways in which suppression methods may be applied are:

a. Line Separation. The need for separating lines through which classified processing is being processed from all other lines should now be fairly obvious. Note that less separation is required when lines come together at right angles than in parallel. A wire inserted in parallel with a conductor makes contact with many lines of force capable of inducing longitudinal currents. The same wire, if turned 90 degrees, will meet perpendicular lines of force which are incapable of such induction, and the two conductors can be safely placed much closer together.

b. Shielding. This method of suppression is extremely important as it is used not only to contain emanations but also to keep those which have been released from coupling back onto conductors. A shield separates two regions so that, in attempting to pass, the electric or magnetic field is attenuated. Most shielding is done by cable shields. However, ferrous and nonferrous foil, conduit, radio-frequency (RF) gaskets, magnetic foil, screens, equipment cabinets, and shielded enclosures are often helpful in suppressing compromising emanations.

c. Bonding. A difference of potential can arise between any two units in an

electrical system, and strong electrical fields are often set up between them. Connecting the points with a low-impedance path (bonding) neutralizes such potential differences. Proper bonding is necessary to produce effective shielding, grounding and filtering.

d. Filtering. Suppressing emanations at or near their source goes a long way toward eliminating compromising signals. Without this suppression, it is still possible for some signals to reach conductors which could carry them to unprotected areas. Since a filter functions to freely transmit signals of certain frequencies while attenuating all others, filtering these lines is often the answer.

e. Acoustical Suppression. Suppressing acoustical emanations presents different sorts of problems; and, where the need exists, totally isolated soundproof rooms are built.

1) Structural Massiveness. The size of facility will go a long way toward isolating sound.

2) Floating Floors. Floors can be built, riding on a resilient quilt of glass or mineral wool, which reduce and isolate vibrations.

3) Wall Covering. Many available porous materials can be used to cover walls. Their absorbent qualities suppress acoustical emanations.

4) Duct and Common Corridor Attenuation. Baffles, cones or acoustical honeycombs of sound-absorbent composition (for example, fiberglass) and configuration may be required for certain air ducts and common corridors. Additional sound attenuation in ducts may be obtained by using flexible (asbestos cloth) sections installed at some point between the TEMPEST source and other areas. Sound traps or silencers of standard manufacture are also available

In summary, we know what a compromising emanation is, some ways it can be generated, and some of the suppression techniques which can be applied to stop these emanations from leaving the secure area. Your Certified TEMPEST Technical Authority (CTTA) can assist by recommending specific selective criteria based on the characteristics of any particular facility.