~~SECRET~~

NSTISSI 7002
17 March 1995

NSTISS
NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY

TEMPEST GLOSSARY

CLASSIFIED BY DIRNSA (NATIONAL MANAGER, NSTISS)
DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED

~~NOFORN~~
~~SECRET~~

~~SECRET~~

NSTISS
NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY

NATIONAL MANAGER

FOREWORD (U)

(U) This Glossary contains definitions of terms associated with TEMPEST, which is a short name referring to investigations and studies of compromising emanations. This glossary supersedes NCSC-3, "TEMPEST Glossary", dated 30 March 1981.

(U) The terms listed and defined herein are those which are directly related to the TEMPEST discipline and could be applied to more than one TEMPEST publication. Engineering and technical terms in common use are not included in this Glossary unless their definitions are altered when these terms are applied to the TEMPEST discipline.

(U) Certain definitions contained herein are classified; the overall classification of the Glossary is SECRET-NOFORN. The classification symbols used for each term are (S), (C), (U), or a combination thereof. The classification symbol following a term or definition indicates its classification. If both the term and definition are unclassified, only the symbol "(U)" follows after the term. Documents in which classified definitions are used must, therefore, be appropriately classified as well.

(U) This Glossary is effective immediately. Users should be directed to obtain additional copies of the Glossary from:

Attn: NSTISSC Secretariat (V503)
National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755-6000

(U) Users should direct comments and recommendations concerning definitions contained in the Glossary to:

Attn: C9
National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755-6000

J. M. McCONNELL
Vice Admiral, U.S. Navy

~~NOFORN~~
~~SECRET~~

~~SECRET~~

TEMPEST GLOSSARY

A

Access (U) - for (COMSEC) applications, access is the capability and opportunity to gain knowledge of or to alter information or material. For Automated Information Systems (AIS) applications, access is the ability and means to communicate with (i.e., input to or receive output from), or otherwise make use of any information, resource, or component in an AIS.

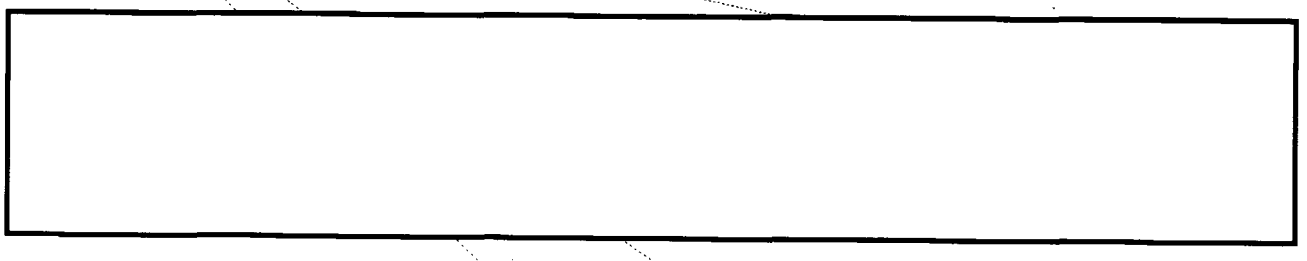
Acoustic Emanation (U) - Emanations in the form of free-space acoustical energy produced by the operation of a purely mechanical or electromechanical device or equipment. Such emanations may be compromising under the definition of "compromising emanations."

Ambient Level (U) - Ambient levels may be classified into two categories: (a) test Environment Ambient Level - those levels of radiated and conducted noise that exist at a specific test location and time when only the equipment under test is inoperative. Atmospherics, interference from other sources, and circuit noise or other interference generated with the test detection system comprise the "test environment ambient level"; (b) Equipment-Under-Test Level - those levels of radiated and conducted noise that originate in the equipment under test and are not compromising emanations.

Ambiguity (U) - A condition that precludes positive identification of specific characters and functions utilizing the parameters of the detected signal. This condition exists when the intelligence related signal emanation can be equated to more than one character or function or groups of characters or functions.

Analog Signal (U) - A signal whose amplitude, phase or frequency content is continuously proportional to the stimulus.

Asynchronous (U) - This word is used in two different ways: (a) a serial system that requires an additional bit or bits for speed adjustment (i.e., latch and release bits); (b) a method of operating the equipment under test or the display equipment that will optimize the probability of signal detection.



B

Baud (U) - The unit of serial signal rate.

Bit (U) - Three definitions are used: (a) a unit interval of time; (b) a binary digit; or (c) the basic unit of information, I(X). If the probability of occurrence of event X is P(X), the knowledge that X has, in fact, occurred is I(X)=-log P(X) bits of information (base 2 logarithms). If P(X) = 1/2, I(X) = 1 bit of information.

Bit-by-Bit Modulation (U) -

(S)

Bit Density Information (U) -

(S)

BLACK (U) - Designation applied to telecommunications and automated information systems, and to associated areas, circuits, components, and equipment, in which national security information is not processed.

BLACK Line (U) - Any line, other than primary or secondary RED conductors, external to national security information processing equipment.

BLACK Signal (U) - Any signal (e.g., control signal or enciphered signal) which would not divulge national security information if recovered and analyzed.

C

Certified TEMPEST Technical Authority (CTTA) (U) - An experienced, technically qualified U.S. Government employee who has met established certification requirements in accordance with NSTISSC-approved criteria and has been appointed by a U.S. Government Department or Agency to fulfill CTTA responsibilities.

Channel Matrix (U) - A two dimensional array of conditional probabilities P(Y/X) where [Y] is the set of received signals and [X] is the set of transmitted signals. This is also called the forward channel matrix. The array of P(X/Y) is called the reverse channel matrix.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Channel Uncertainty (U) - See Uncertainty.

Code (U) - System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length.

Compromise (U) - Disclosure of information or data to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Compromising Emanations (CE) (U) - Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled or otherwise processed by telecommunications or automated information systems equipment.

Conducted Signals (U) - Electromagnetic or acoustic emissions of undesired signal data which become induced and propagated along wire lines or other conductors.

~~SECRET~~

Confidence Interval (U) - A range of values that contain the true value with a selected probability called the confidence level.

Control Line (U) - Line intended for the transmission of control signals, alarm indicators and fault determination between components of a system.

Correlated Emanations (CORR E) (U) - Detected emanations which correspond to or contain a discernible relationship to any signal or process of known characteristics. Correlated emanations may be compromising under the definition of "compromising emanations."

Countermeasure (U) - Action, device, procedure, technique, or other measure that reduces the vulnerability of any equipment that electronically processes information.

Cycle (U) - The total number of bits (synchronizing, intelligence, error checking, or control bit) required to transmit any given character in a serial communication system.

D

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403

Data Related Emanations (DRE) (U) - Detected emanations which have a discernible relationship with a signal related to the data processed by the EUT, and have been analyzed and determined to be not compromising.

Deterministic Channel (U) - A channel where each input is converted to one and only one output. Such a channel can be characterized by a channel matrix with one and only one nonzero element in each row. Note: The inverse (each output represents only one input) is not necessarily true.

Digital Signal (U) - A nominally discontinuous electrical signal that changes from one state to another in discrete steps.

[redacted]

Digraphic Information - (U) [redacted]

Digraphic Processing (U) - Processing where the data (bits) are parallel processed, and the characters are processed two at a time.

Dry Line (U) - An interface line of the equipment under test which does not normally carry a signal or from which the normal signal has been removed.

E

Electric Radiation (ER) (U) - That portion of an electromagnetic field that is caused by a difference in potential.

Electromagnetic Field (U) - Energy that exists in the vicinity of a conductor of electricity. It consists of Electric Radiation and Magnetic Radiation components.

Emanation (U) - Unintended signals or noise appearing external to an equipment.

Entropy (U) - See Uncertainty.

Equipment Radiation TEMPEST Zone (ERTZ) (U) - A zone established as a result of determined or known equipment radiation TEMPEST characteristics. The zone includes all space within which a successful intercept of compromising emanations is considered possible.

Equipment Under Test (EUT) (U) - An equipment or group of equipments subjected to TEMPEST testing.

EUT Exerciser Equipment (U) - Any equipment or device (not part of the EUT) used during TEMPEST testing to make the equipment under test (EUT) operate; e.g., a similar or complementary equipment for back-to-back operation or an external clock source. This term may be used interchangeably with EUT stimulus equipment.

Event (U) - There are two definitions: (a) a noteworthy happening; (b) a subset of the possible outcomes in a future experiment. Many analysis concepts inherit this subtle duality and have a different meaning before and after an event has occurred.

F

Facility (U) - A physically definable area consisting of inspectable space which contains national security information processing equipment.

Fingerprint Signal (U) - A unique emanation caused by the processing or transfer of an information unit (e.g., character, byte, etc.) by the EUT (also called signature).

Fortuitous Conduction (U) - Emanations in the form of signals propagated along any unintended conductor.

Fortuitous Conductor (U) - Any conductor that may provide an unintended path for signals. Fortuitous conductors include cable, wires, pipes, conduits and structural metal work in the vicinity of a radiation source.

Format (U) - An aspect of entropy that doesn't depend on language but rather on how messages are structured.

Full Bit Emanation (U) - An emanation that correlates on a one-to-one basis with the bits of the message code signal.

G

Generatrix (U) - The set of characters that are considered to be the cause of a particular received TEMPEST signal, arranged in order of probability.

~~SECRET~~

Generatrix Family (U) - The groups (sets of generatrices) into which the characters of the alphabet are assigned by the TEMPEST encoder. Also, the groups into which the characters are assigned at the output of the detector for analysis purposes.

Generatrix Sequence (U) - The sequence of generatrices resulting from a test where a representative test message for the EUT is processed. One generatrix is generated for each received signal.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

H

HIJACK (U)

~~(S)~~

I

Impulsive Emanation (U) - An emanation composed of impulses.

Information Ratio (IR) (U) - A measure of the amount of information which can be derived from a detected signal. It is the ratio of the amount of information contained in a signal to the amount of information necessary for 100 percent recovery of plain text information.

Inspectable Space (U) - The three dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and/or remove a potential TEMPEST exploitation exists.

K

Knowledge (U) - The fact or condition of being aware of an event.

L

Latch or Stop Bit (U) - A bit that serves to bring the receiving mechanism of a serial processing equipment to rest in preparation for the reception of the next character.

Line Conduction (U) - Unintentional signals or noise induced or conducted on a telecommunications or automated information system signal, power, control, indicator or other external interface line.

M

Magnetic Radiation (MR) (U) - The component of the electromagnetic field that is caused by current flow.

Mark (U) - This is the serial signal condition when the equipment under test is in an energized (current flow) condition or when there is a change in the polarity of the signal.

Monitor Signal (U) - The signal to which a detected emanation is compared for determining correlation; a monitor is usually a RED signal.

Monographic Information (U)

(c)

Monographic Processing (U) - Processing where each character is sequentially processed in a bit parallel format.

Multichannel Information (U) - Information which results when emanations from multiple TEMPEST channels are used to extract information correlating to a single message being processed.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

~~SECRET~~

N

National Security Information (U) - Information that has been determined, pursuant to Executive Order 12356 or any predecessor order, to require protection against unauthorized disclosure, and that is so designated.

Noise (U) - Disturbances superimposed upon a signal that tend to obscure its information content.

NONSTOP (U)

~~(S)~~

Nontunable (U) - A term used to describe a test, or test instrumentation, in which frequency coverage is selected in one or more discrete increments; i.e., not continuously variable. Nontunable detection systems do not contain a demodulator.

P

Parallel Information Unit (U) - Two or more bits arranged in a deterministic order which are transferred to be stored simultaneously as a unit. One parallel information unit is transferred when a clock or trigger pulse causes the entire unit to be simultaneously gated out of a register or other storage device. Two or more units can form a larger unit.

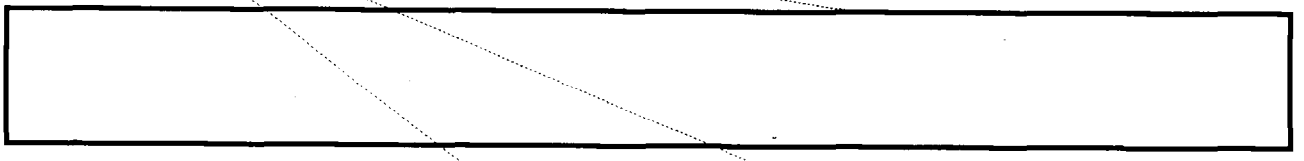
Polygraphic Information (U)

~~(C)~~

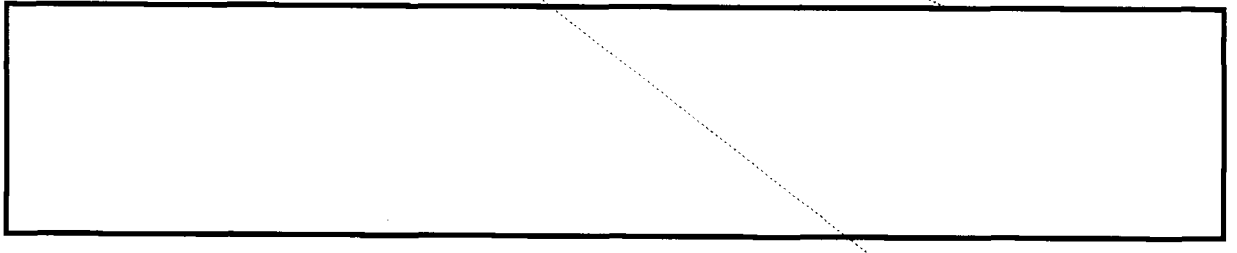
Polygraphic Processing (U) - Processing where the data (bits) are parallel processed more than one at a time.

~~(S)~~

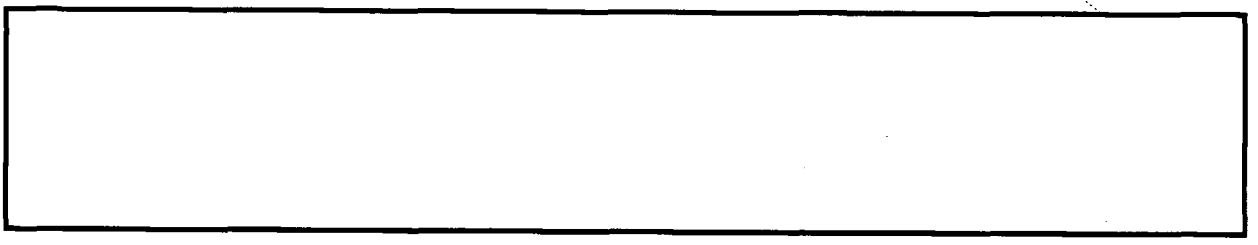
~~NOFORN~~
~~SECRET~~



Power Line Conduction (U) - See Line Conduction.



Primary Red Conductor (U) - Any conductor intended to carry national security information and terminating in RED equipment or in the RED side of crypto-equipment or isolation devices.



Probability (U) - The relative frequency of occurrence of a given event out of all possible events. Alternately stated, the change that an event will occur, measured as the ratio of the noteworthy outcomes to the total number of outcomes.

R

Radiated Signal (U) - Electromagnetic or acoustic emissions of undesired signal data which are propagated through space.

Radiation (U) - Signals emanating from an equipment which appear as either electromagnetic fields or as spatial longitudinal waves. These include induction field, magnetic field, electric field gradient and acoustic waves.

Recoverable Zone (U) - The three dimensional space surrounding an equipment or system processing national security information within which it is theoretically

possible to recover the information processed. For radiated signals, this term may be used interchangeably with Equipment Radiation TEMPEST Zone (ERTZ).

RED (U) - Designation applied to telecommunications and automated information systems, and to associated areas, circuits, components, and equipment in which national security information is being processed.

RED/BLACK Concept (U) - Separation of electrical and electronic circuits, components, equipment, and systems that handle national security information (RED), in electrical form, from those which handle non-national security information, (BLACK) in the same form.

RED Line (U) - A primary or secondary RED conductor.

RED Signal (U) - Any signal (e.g., plain text, key, key stream, subkey stream, initial fill or control signal) which would divulge national security information if recovered.

Rd (U) - RED analog signaling or RED pulse width signaling rate or RED digital signaling rate.

Rt (U) - RED transmission time signaling rate.

Release or Start Bit (U) - A bit that serves to prepare the receiving mechanism of an equipment for the reception and the registration of a character.

S

Secondary RED Conductor (U) - Any conductor, other than primary RED, which connects to RED equipment, the RED side of crypto-equipment, or the RED side of isolation devices, which does not intentionally carry national security information; but because the coupling mechanism with the RED equipment might carry compromising information, is designated secondary RED (e.g., indicator lines, control lines, timing lines, etc.). Power distribution panels and grounding systems serving RED wire lines and equipments may also be so designated.

Seismic Emanation (U) - Emanations in the form of structural vibration energy produced by the operation of a purely mechanical or electromechanical device or equipment.

Serial Signal (U) - A signal where information is conveyed by the time relationships of bits, i.e., bits are transferred one at a time in a specified manner.

Short Cycle Operation (U)

(e)

Signal (U) - A fluctuating quantity, such as voltage, current, electrical field strength, sound pressure level, etc., the variations of which convey information.

Signal Bandwidth (U) - That portion of the frequency spectrum which must be passed by signal processing equipment in order to minimize signal distortion.

Skewed Parallel Signal (U)

(e)

Space (U) - This is the serial signal condition where the equipment under the test is in an unenergized (no current) condition (as opposed to Mark). Note: This is not the definition of the space character.

Space Radiation (U) - The phenomena in which electromagnetic or acoustic signals emanate from an equipment under test into free space.

Standard Measurement Point (U) - The point where the compromising emanation performance requirement (CEPR) applies. For an electric or magnetic field emanation, the standard measurement point is one meter from the equipment under test. For a conducted emanation, the standard measurement point is at the design radius.

Synchronous (U) - A system that does not require an additional bit or bits for speed adjustment, i.e., latch and release bits.

~~SECRET~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

T

TAILSPIN (U) [redacted] ~~(S)~~

Telecommunications (U) - Preparation, transmission, communications, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical or electronic means.

TEMPEST (U) - A short name referring to investigation, study and control of compromising emanations from telecommunications and automated information systems equipment.

TEMPEST Advisory Group (TAG) (U) - A permanent subcommittee of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) established to serve as a national level forum for TEMPEST matters of mutual interest to the membership in support of the U.S. Governments TEMPEST security objectives.

TEMPEST Channel (U) - An unintentional communications channel which conveys information about the information processed through the intentional communications channel.

TEMPEST Encoding (U) - An unintentional process which results in the altering of information before it is emitted into the TEMPEST channel.

TEMPEST Test (U) - A laboratory or on site (field) test to determine the nature and amplitude of conducted or radiated signals containing compromising information.

Test Detection System (U) - The instrumentation used in performing a TEMPEST test including the transducer, detector, display devices, recording devices, filters, coaxial switches, etc.

Test Message (U) - A series of characters or signals chosen to be processed by the equipment under test during TEMPEST testing.

~~NOFORN~~
~~SECRET~~

Time Correlated Pulse (U) - A pulse that occurs at exactly the same time in the character cycle each time a particular character is processed by the equipment under test during TEMPEST testing.

Transition Density Information (U)

~~(C)~~

Transitional Signal (U) - In the TEMPEST channel, the impulse that occurs at the time of a change from one signaling condition to another such as the change from "mark-to-space" for from "space-to-mark."

Tunable (U) - A term used to describe a test, or test instrumentation designed to cover a fixed frequency range in continuous or stepped contiguous (within the specified bandwidth) increments. Tunable detection systems may contain a demodulator.

U

Uncertainty (Entropy) (U) - Two definitions are used: (a) the average amount of information gained per received signal; (b) the average amount of information required before one is certain that an event has occurred. The types of Uncertainty are:

(1) Input Uncertainty (H(X)) - This is the average amount of information provided by the source language.

(2) Output Uncertainty (H(Y)) - This is the average amount of information provided by the received signal.

(3) Forward Channel Uncertainty (H(Y/X)) - This is the average amount of information required to be certain what signal will be received if the transmitted symbol is known.

(4) Reverse Channel Uncertainty (H(X/Y)) - This is the average amount of information required to be certain what symbol was sent if a certain channel output is observed.

(5) Transinformation or Information Gain (I(X/Y)) - This is the average information that is obtained about which symbol was transmitted if the channel output is observed and the source language statistics are known.

W

Wet Line (U) - An interface line of the equipment under test, where the signal normally transmitted over the line is present.

DISTRIBUTION:

EXEC REG
C/S
AGC/I
ADIL
GC
B03
C/SCI (2)
C
C6
C7
C9
F1A
F1C
F1D
F1E
F1F
F1G
F1H
F1I
F1L
F1M
F2 (5)
F32
F321
F33
F34
F38
F4 (5)
F41
F45
F47
F6
F81
F83
F91
F92
F92 (Vital Records)
G
I
I04
I044
I2
I1
I1/S
I11
I9

J
J C/S
J06
J3
K
K509
K511
L06
M509
M51
M52
NSALO/DISA
N5
N51
N52
P
P04
P1
P6
Q3
R
R2
R23
R7
R8
T09
V
V1
V2 (9)
V3
V4
V49 (5)
V5
V503
V51
V52
V53
V6
V7
Y
Y1
Y106
Y13 (6)
Y134
Y2 (21)
Y4
NSTISSC Secretariat (50)