Computer Security

Access— the ability and means to approach, communicate with (input to or receive output from) or otherwise make use of any classified material or any component of an automated data processing (ADP) system.

Access control— operational procedures and physical security measures designed to limit the availability of either classified ADP data in any form, or physical ADP resources, to a recipient.

ADPE— abbreviation for automated data processing equipment.

ADP system damage minimization efforts— efforts and resources whose purpose is keeping to a minimum the ADP dollar loss, adverse impact on ADP, and supported agency operations. Damage minimization efforts can be identified as belonging to system backup, control and warning systems, and drills.

ADP system threat— any danger to ADP installations, hardware, software, communication links, inputs/outputs, or data which could adversely affect ADP system performance, accomplishment of the DPI mission, or ADP system security. They are (human error, sabotage, and theft), accidental, and natural disasters; DPI environmental degradation; and ADP equipment failure threats.

ADP system threat minimization efforts— the sum of hardware and software features, physical and personnel resources, and operating and administrative procedures designed to prevent or minimize the probability of that occurrence. They include physical security measures, personnel training, personnel security procedures, equipment reliability, data security, and communications security (COMSEC).

ADP system security— the hardware/software functions, characteristics, and features; operation procedures, accountability procedures, and both access and entry controls at

the central computer facility, remote computer and terminal facilities; management constraints, physical structures, and devices; and personnel and communications controls needed to provide an acceptable level of protection in a computer system.

Audit— a system for tracing items of data from processing step to processing step, particularly from a machine-produced report or other machine output back to the original source data.

Automatic data processing (ADP)— any phase of data recording, manipulation, remote terminal operations, and other related operations in which data are processed by ADPE; systems inclusive of punched card machines (PCM) and terminal operations.

Backup system— a compatible ADPE configuration at an alternate site which will effectively process mission essential ADP applications in case of damage, environmental disruption, or equipment malfunction.

Breach— successful defeat of security controls that could result in penetration of the system. Examples include, but are not limited to, operation of user code in control program mode, unauthorized acquisition of ID password or file access passwords, and not using prescribed operating system mechanisms to gain a file.

Data— information or symbology contained in storage, registers, buffers, documents, cards, tapes, drums, and communications links.

Data processing (DP) installation/ activity (DPI/A)— any facility, room, or building housing ADPE, storing tapes, cards, or other media used to perform the ADP support mission. It does not include the housing of auxiliary power sources, or output processing areas (unless they are collocated with the DPI/A). A DPA, by nature of its mission and resources, can function independently within the DPI. It normally has a separate manager and a separate ADPE configuration.

Data security— protection of data from either accidental or unauthorized modification, destruction, or disclosure; sabotage; malicious; mischief; theft; or mutilation.

Debug/test program procedures— methods used to locate and correct any errors in a computer program.

Disaster— an occurrence that could completely prevent a DPI from accomplishing its normally assigned mission. (This includes fire, major water damage, extended power failure, sabotage, etc.).

DP equipment malfunction— temporary failure of any equipment to function as designed when required.

Drills— simulations designed to test the performance of resources, systems, procedures, and personnel against standards established for threat minimization.

Edit controls— measures designed to identify rearrangement of data or information. The editing may involve deletion of unwanted data, selection of pertinent data, and the testing of data for reasonableness and proper range.

Entry— the ability and means to approach, communicate with (input to or receive output from), or otherwise make use of either unclassified material or any component of an automated data processing system.

Entry controls— operational procedures and physical security measures designed to limit availability of either unclassified ADP data in any form, or physical ADP resources, to a recipient.

Environmental disruption— improper concentrations of rust, dust, humidity, smoke, temperature, foreign matter, etc., in a room housing ADPE.

Erase/degauss procedure— a protective measure that involves overwriting or rerecording on a magnetic surface so as to

completely erase the original data.

ESI— abbreviation for especially sensitive information.

Human error— unintentional act of a human that results in the occurrence or probable occurrence of a disaster, environmental disruption, or equipment malfunction; or the unintentional addition, deletion, or substitution of data in any file, record, or program.

Inputs/outputs (I/O)— physical media processing information used as an input or output in an ADP system. (Includes documents, punch cards, magnetic tape, punched tape, machine printouts, and similar media. Excludes the data or information displayed or the information on the media.)

MISM— abbreviation for management information system material.

Multilevel security mode— a mode of operation under an operating system (supervisor or executive program) which provides a capability permitting various levels and categories or compartments of material to be concurrently stored and processed in an ADP system. In a remotely accessed resource-sharing system, the material can be selectively accessed and manipulated from variously controlled terminals by personnel having different security clearances and access approvals. This mode of operation can accommodate the concurrent processing and storage of two or more levels of classified data, or one or more levels of classified data with unclassified data depending upon the constraints placed on the systems.

Operating system— an integrated collection of service routines for supervising the sequencing and processing of programs by a computer.

Passwords— a word or string of characters, uniquely associated with a use, which either authenticates a user or identifies a defined system resource, such as a program.

Penetration— a successful unauthorized entry and/or access into a system.

Physical security measures— protective actions against threats to the central computer facility, its remote computer and terminal facilities, the related tape/disk libraries, and the supporting areas achieved by locks, guards, badges, personnel security clearances and administrative control measures outside the computer as well as measures required for the protection of the structures housing the computer. Associated with these measures should be provisions for off-site storage of data and for backup systems.

Remote terminals— remotely located devices used to input data to and receive output data from a central computer system by communication lines or cables. Generally, these devices are physically located in an area separated from the central site.

Remotely accessed/entered resource sharing computer system— a computer system that includes one or more central processing units, peripheral devices, remote terminals, and communications equipment or interconnection links, which allocates its resources to one or more users, and which can be used from terminals located outside the central computer facility.

Resource sharing computer facility— a computer facility that uses its resources, including I/O devices, storage, central processor (arithmetic and logic units), control units, and software processing capabilities to enable two or more users to manipulate data ‘and process coresident programs in an apparently simultaneous manner. The term includes systems with one or more of the capabilities commonly referred to as time-sharing, multiprograming, multiaccessing, multiprocessing, or concurrent processing.

Routine, utility— a standard routine used to assist in the operation of the computer, such as a conversion routine, a sort routine, or a printout routine.

Sensitive information— unclassified data which a commander designates for special handling, including individuals authorized to receive it.

SIOP— abbreviation for single integrated operational plan.

Software lockout— prohibition of access to information through programing techniques rather than hardware lockout or physical means.

System backup— a computer or peripheral equipment normally specifically designated and available to provide computer processing/services if the primary computer system or its peripherals are destroyed or otherwise unavailable. Backup equipment may be collocated with the primary system or at another installation.

Tempest— refer to AR 530-4.

Warning system— any device or procedure designed to alert personnel to a specified event or threat.

Intrusion Detection Systems (IDS)

Actuator— in commercial security systems, a holdup button, magnetic switch or thermostat that will cause the system to alarm.

Annunciator (monitor)— a visual or audible signaling device that indicates conditions of associated circuits. Usually, this is accomplished by activation of a signal lamp and audible sound.

Antenna— a conductor or system of conductors for radiating or receiving electromagnetic waves.

Balanced magnetic switch— a magnetically operated switch designed to detect the opening of a secured door, window, or other closure. In addition, it detects attempts to defeat the switch by substituting a magnetic field and may have provisions for internal adjustments and detection of switch tampering attempts.

Capacitance— the property of two or more objects which enables them to store electrical energy in an electrostatic field between them.

Capacitance proximity sensor— records a change in capacitance or electrostatic fields to detect penetration through windows, ventilators, and other openings, and can be used to detect attempted penetration into safes or storage cabinets.

Conductor— material which transmits electric current. Wire and cable are conductors. Also called signal transmission lines.

Contacts— parts of a switch or relay which by touching or being separated permit electric current to flow or cease to flow. Frequently and improperly used to designate an entire magnetic switch or balanced magnetic switch component.

Control unit— the terminal box for all sensors. It receives alarm and tamper signals and transmits these signals to the local audible alarm and/or monitor unit. It provides the primary and backup power for all sensors; activates and deactivates the system.

Data transmission system— Component consisting of a data transmitter in the control unit and a data receiver in the monitor unit and is the communication link used to pass alarm and equipment status signals from the control unit to the monitor unit over a wire transmission line or by radio frequency.

Doppler— the effect of compression of expanding sound or radio frequencies reflected from or originating from a moving object.

Fail-safe— a term applied to a system designed so that if a component fails to function properly, the system, will, by a

signal or otherwise, indicate its incapacity.

False alarm— activation of sensor(s) for which no cause can be determined.

Fixed duress sensor— an emergency notification device, switch, or button manually operated by personnel needing assistance.

Grid wire sensor— detects forced entry through walls, floors, ceilings, doors, and other barriers by the break-wire method.

Intrusion detection system— the combination of components, including sensors, control units, transmission lines, and monitor units integrated to operate in a specified manner.

Intrusion detection sensors— devices that initiate alarm signals by sensing the stimulus, change, or condition for which they were designed.

Joint-Service Interior Intrusion Detection System (J-SIIDS)— developed as a standard detection system for joint-service application for protection of military arms rooms and other inside areas.

Local audible alarm— an electronic screamer or bell for outdoor or indoor use in the vicinity of the protected area.

Magnetic contact/simple magnetic switch— consists of two separate items, a magnetically actuated switch and a magnet. The switch is usually mounted in a fixed position (door frame or safe) opposing the magnet, which is fastened to a hinged or sliding door. When the movable barrier is opened, the magnet moves with it and the switch opens. Magnetic contacts are usually connected so that the switch is closed while the magnet is near. This allows the electric current to flow. When the door or window is open, the magnetic contact opens. This stops the electric current flow, causing an alarm.

Magnetic weapon sensor— a wire loop assembly used to detect the magnetic field disturbance caused by the removal of a weapon from a weapons rack.

Microwave sensor— a radio/radar frequency (RF) transceiver having a frequency range of GHz (billion cycles per second) which detects motion through the Doppler shift effect.

Monitor— a device that senses and reports on the condition of a system, commonly used interchangeably with the terms, monitor unit, monitor panel(s), status indicator module, annunciator, and other similar terms.

Motion sensor— detects movement inside the area to be protected.

Nuisance alarm— the result of a sensor activation caused by accident, neglect, malfunction, or natural causes, such as wind, lightning, or thunder. Often improperly called false alarm.

Overload— a condition in which an electrical device draws a current greater than its rated capacity.

Passive ultrasonic sensor— detects the sounds of forced entry through walls, ceilings, and doors.

Penetration sensor— detects entry through doors, windows, walls, or any other openings into the protected area.

Photoelectric system— usually supplied as two separate units, a transmitter and receiver. A light beam is transmitted to the receiver. Any interruption of this light causes an alarm.

Point sensor— detects removal or attempted removal of an object from its storage container.

Radio— radio frequency (RF) transceiver having a frequency range of 100 MHz (million cycles per second) to 1 GHz (billion cycles per second).

Sonic— having a frequency within the hearing distance of the human ear.

Supervised line— a conductor which (if cut, broken, shorted, or otherwise tampered with) will cause a change in status indicated at a monitoring unit.

Telephone dialer— a device, normally installed within the protected area, that automatically dials preselected telephone numbers upon sensor activation and provides a prerecorded message notifying of intrusion.

Ultrasonic— the frequency range of sound that is above the capabilities of normal human hearing. In intrusion detection systems it usually varies between 21,500 and 26,000 Hz (cycles per second).

Ultrasonic motion sensor— detects by frequency shift (doppler) the motion of an intruder inside the protected area.

Vibration sensor— detects forced entry through metal barriers placed over windows and ventilators or attempts to drill, saw, or cut through walls, ceilings, floors, or doors.

Nuclear Reactors

Access-close physical proximity to special nuclear material, control consoles, or the reactor, which provides the opportunity for tampering with or damaging the material, consoles, or reactor. Posts must be established to control access.

Exception— permanent exclusion from specific requirements based on case-by-case determination that unique circumstances at a given unit, facility, or installation are such that conformance to established standards and measures is impossible, highly impractical, exceptionally costly, unnecessary due to measures exceeding those prescribed, or not in the best interest of the US Government.

Nuclear reactor— a facility in which fissionable material is used in a self-supporting chain reaction (nuclear fission) to produce heat and/or radiation for both practical application and research and development (AR 310-25). A nuclear reactor system includes reactors and their associated components, auxiliary systems, and engineered safeguards.

Nuclear reactor facility— a nuclear reactor system, the associated buildings, auxiliary equipment, and reactor staff required for its operation, maintenance, and support. The term includes both power and research nuclear reactor facilities.

Reactor commander— chief of the organizational unit directly responsible for operation of a nuclear reactor facility, including the reactor staff.

Response force— personnel, other than those performing security functions at the facility, whose mission is to augment the security force as required.

Responsible commander— the organizational element commander or director to whom the reactor commander reports.

Restricted or vital area— any area, designated by the reactor facility commander, to which access is restricted or controlled for reasons of security or to safeguard property or material.

Limited area— a restricted area that surrounds one or more exclusion or vital areas.

Exclusion/vital area— a restricted area which contains special nuclear material, a nuclear reactor, or control consoles.

Security force— personnel performing security duties at the nuclear reactor facility.

Special nuclear material (SNM)— plutonium, uranium enriched in the isotope 233 or in the isotope 235; any other material which the US Nuclear Regulatory Commission determines to be special nuclear material; or any material artificially enriched by any of the foregoing. SNM does not include source material.

Waiver— a temporary exemption, for not more than 1 year, from a specified requirement. (Requests for waivers or exceptions referred previously will include circumstances requiring the action and compensatory measures taken to achieve a comparable degree of security. Requests will be forwarded through command channels to HQDA.)