# Chapter 2
# Security Boundaries

## Introduction

Security boundaries exist at several layers within any secure processing or classified facility. Three boundaries are normally identified, physical, administrative, and emissions. Within the physical and administrative boundaries, two classes exist: stand-alone and networked. The following addresses generic boundaries and related information applying to most systems.

***WHAT ARE SECURITY BOUNDARIES?***

***Security boundaries represent the zone of containment beyond which control of information cannot be maintained.***

The overall security boundary of any system is controlled by access. Access is defined as the ability and opportunity to obtain knowledge or classified information or to be in a place where one could be expected to gain such knowledge. Security measures are implemented to prevent access to protected information using a variety of techniques and controls, including communications security, ADP security, physical security, and TEMPEST emission protection.

***BOUNDARY LAYERS***

***Security boundaries exist at several layers within any secure processing or C3I facility.***

***Three boundaries are normally identified, physical, administrative, and emissions.***

***Within the physical and administrative boundaries, two classes exist: stand-alone and networked.***

Nearly all security measures involve physical controls. Still other measures involve the use of special equipment such as Firewall protected networks, TEMPEST emission protected equipment, COMSEC encryption devices, or trusted computers. Communications security is the protection resulting from all measures designed to deny unauthorized persons access to information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretations of the results of such possession and study. Therefore, there is a certain amount of overlap between each of the security techniques and control functions, regardless of the specific discipline involved. This overlap is pronounced when equipment is connected within a network.

***BOUNDARY ATTRIBUTES***

***The overall security boundary of any system is controlled by access.***

***Nearly all boundaries involve some form of physical security.***

***Some require special hardware.***

***ADP systems require software and, in the case of networks, controlled gateways.***

## Physical Boundaries

For a network of secure processing equipment connected to other networks using COMSEC controlled channels, the boundaries on a system

relate to the environment where processing takes place. To understand this environment, the concept of RED/BLACK isolation is presented. Electrical and electronic circuits, components, equipment, systems, or areas which handle classified plain-language information in electric signal form (RED) are separated from those which handle encrypted or unclassified information (BLACK).

In the network environment, physical boundaries exist at all layers from the external facility design to the circuit board level. Starting at the facility level, the complete building or facility area under direct physical control is considered the Controlled Access Area (CAA). This area can include one or more Limited Exclusion Areas, Controlled BLACK Equipment Areas, or any combination thereof.

The Limited Exclusion Area (LEA) depicted in Figure 1 is a room or enclosed area to which security controls have been applied to provide protection to a RED information processing system's equipment and wire lines. The level of protection must be equivalent to that required for the information transmitted through the system.

A LEA must contain a RED equipment area but can also include BLACK equipment. A Controlled BLACK Equipment Area (CBEA) is a BLACK Equipment Area which is not located in a Limited Exclusion Area but is afforded the same physical entry control which would be required if it were within a LEA.

Controlled Space (CS) is the three-dimensional space surrounding equipment that processes national security information within which unauthorized personnel are (1) denied unrestricted access and (2) either escorted by authorized personnel or are under continual physical or electronic surveillance

***PROTECTED DISTRIBUTION SYSTEM***

***A PDS is a telecommunications system to which electromagnetic and physical safeguards have been applied to permit secure transmission of unencrypted classified, information.***

***Major components are lines (wire or fiber optic), subscriber sets, and terminal equipment.***

***PHYSICAL BOUNDARIES***

***For a network of secure processing equipment connected to other networks, the boundaries on a system relate to the environment where processing takes place.***

***Circuits, components, equipment, systems, or areas which handle classified plain-language information in electric signal form (RED) are separated from those which handle encrypted or unclassified information (BLACK).***

***TEMPEST boundaries relate to the emission detection distance from the protected equipment.***

***CONTROLLED BLACK EQUIPMENT AREA***

***A BLACK Equipment Area which is not located in a LEA but is afforded the same physical entry control.***

***Controlled Space (CS) is the three-dimensional space within which unauthorized personnel are (1) denied unrestricted access and (2) either escorted by authorized personnel or are under continual surveillance***

A Protected Distribution System (approved circuit) is a telecommunications system to which electromagnetic and physical safeguards have been applied to permit secure transmission of

unencrypted classified, information and which has been approved by the department or agency responsible. The associated facilities include all equipment and lines so safeguarded. Major components are lines (wire or fiber optic), subscriber sets, and terminal equipment.

**Emission Boundaries**

A compromising emanation is an unintentional data-related or intelligence-bearing signal which, if properly intercepted and analyzed, can disclose the classified information transmitted, received, handled, or otherwise processed by information processing equipment. Protection techniques to reduce the threat posed by emanations include the use of protected equipment, shielded facilities, or protected radiation zones. TEMPEST equipment is RED equipment that has employed special control techniques which reduce the equipment's radiated emissions to accepted levels. COMSEC equipment incorporates TEMPEST emission controls, and provides for encrypting data for transmission to other locations.

For facilities where non-TEMPEST equipment is utilized, the emission control requirements do not change, only their means of implementation. The Equipment TEMPEST Radiation Zone (ETRZ) is a zone established as a result of determined or known equipment TEMPEST radiation characteristics. The zone includes all space within which a successful hostile intercept of compromising emanations is considered possible.

**Network Emission Boundaries**

When equipment is networked over a larger area in a single facility, some emission problems occur that were not obvious in the stand-alone environment. Many requirements documents deal with the proper isolation of facilities and their secure processing capabilities. The documents, such as MIL-HNBK 232, NACSEM 5109, NACSEM 5111, and NACSEM 5203, and DIAM 50-3 and 4 provide guidance and verification criteria. However, it still falls upon the responsible security professional to determine the unique techniques and the proper application of principles to be employed at each individual location. Not only must the specific computer related or electromagnetic effects discipline be considered, but all the various inter-related security problems must also be considered.

The United States Army Corps of Engineers has identified and cataloged a number of subsystems supporting facility and ground requirements for secure processing facilities[1]. Identified subsystems include utilities, heating, ventilation, and air conditioning (HVAC), earth electrode, lightning protection, communications, computing and data processing control, signal security, and personnel support equipment. The problem associated with these various subsystems in secure facilities is their

***SUBSYSTEM BOUNDARIES***

***The US Army Corps of Engineers has identified and cataloged a number of subsystems supporting facility and ground requirements for secure processing facilities.***

***Identified subsystems include utilities, HVAC, earth electrode, lightning protection, communications, computing and data processing control, signal security, and personnel support equipment.***

[1] H.W. Denny, T.G. Shands, R.G. McCormack, and J.A. Woody, "Integrated Grounding and Bonding Practices in Command, Control, Communications, and Intelligence Facilities," USA-CERL Technical Report M-89/01, October 1988.

interactive effect on the specific protection control installed for specific systems. The following information, some of which was extracted from the Corps of Engineers report, describes the computer and data processing subsystem.

***COMMUNICATIONS SUBSYSTEM***

***Considered the network of electronic equipment, interfaces, and antennas whose elements are located in and around the C3I facility.***

***The purpose is to transfer information from one point to another using various protected and non-protected means.***

***The protected transmission paths employ shielded twisted pair, coaxial cables, or fiber optics.***

**Communications Subsystem**

The communications subsystem is the network of electronic equipment, interfaces, and antennas whose elements are located in and around the C3I facility. The purpose of the communications subsystem is to transfer information from one point to another. Within the facility, information is generally transferred over hard-wired signal lines using various protected and non-protected means. Between facilities, secure information transfer is encrypted and generally not a problem.

An important, secure communication subsystem is that associated with high-speed data transmission. This subsystem is used to transfer high-speed data signals between data processing equipment. The protected transmission paths employ shielded twisted pair, coaxial cables, or fiber optics.

The equipment of the various communication elements is likely to be distributed throughout the facility and grounded at multiple points. The equipment cases, racks, and frames are grounded to the ac power ground, raceways and conduits, and structural members at numerous locations within the facility. In many facilities, a single point configuration for the signal reference ground is said to be implemented for telephone circuits and data processing circuits. Actually, however, a single-point ground configuration does not exist because of internal grounding of signal references to cabinets and enclosures with subsequent interconnections to power conduits and raceways and because of unbalanced interfaces between the various pieces of equipment. Consequently, the effective signal reference ground for the communication subsystem in the typical C3I facility is a multipoint grounded system with numerous interconnections between signal references, equipment enclosures, raceways, conduits, and structural members.

**Computing and Data Processing Subsystem**

A distinguishing feature of the C3I facility is the presence of many digital processors ranging from microcomputers performing dedicated equipment and instrument control to large interconnected mainframes providing complex analyses, signal processing, and image displays. These processors typically interface with numerous I/O (input/output) devices including keyboards, monitors, disk drives, tape drives, remote terminals, data acquisition and control equipment, and other processors.

The data processing subsystems are configured in various ways. These configurations result in a myriad of different grounding connections being established. For example, stand-alone desktop computers obtain power from single ac outlets and thus establish only one electrical

safety ground connection. Other small computing systems may be configured so that the processor and I/O devices share the same outlet or perhaps the same branch circuit. In this configuration, the ground connection is effectively a single connection, although more than one physical tie is made. Where I/O and other peripherals are separated by large distances from the processor, multiple connections to the facility ground network will result.

***INTERCONNECTION RULES***

***If a network consists of previously accredited AISs, a MOA is required between the DAA of each DoD Component AIS and the DAA responsible for the network.***

***Connections between accredited AISs must be consistent with the mode of operation of each AIS, the specific sensitivity level or range of sensitivity levels for which each AIS is accredited, any additional interface constraints associated with the particular interface device used for the connection, and any other restrictions required by the MOA.***

***Untrusted, unaccredited AISs, either individual computer systems or sub-networks, also may be components of a network.***

Larger computing subsystems are generally characterized by having the processor in one place and the peripherals distributed throughout the facility. In this configuration, the peripherals are supplied from different ac outlets, off of different branch circuits, or perhaps from different phases of the powerline. In some installations, remote terminals may even be in separate buildings and supplied from different transformer banks. Each remote device must have a safety ground at its location.

Noise in interconnecting paths can be encountered from stray currents in the ground reference network. The most practical approach to solving these noise problems is not to strive to implement a single-point ground connection for the main processor but rather to minimize the stray current in the ground reference system and use effective common-mode suppression techniques and devices in data paths.

## The Network Boundary

Since and AIS is not in many cases composed of a single computer system, the boundary of the AIS often becomes blurred within the data processing subsystem. An AIS may consist of many computers and peripherals of various sizes that work together in support of a single function.

***AIS BOUNDARIES***

***In modern networked environments, AIS boundaries are difficult to establish.***

***AIS boundaries may exist at the equipment level, LAN level, LAN/LAN level, or LAN/WAN level or may also relate to ownership or control of equipment, or to the information processed by the equipment.***

***THE SINGLE FUNCTION THEORY***

***The single function theory forms the basis for defining the boundaries of an AIS.***

***Any computer system which shares functionality between the classified LAN and other non-classified functions is defined as a single AIS in and of itself.***

The single function theory forms the basis for defining the boundaries of an AIS. For example, in the Marine Corps, any computer system used exclusively for supporting the WIN function forms a part of the WIN AIS. Any computer system which shares functionality between the WIN and other non-classified functions is defined as a single AIS in and of itself. Section 6.0 and the sections that follow discussed interconnection requirements between AIS boundaries.

**Signal Security Subsystem**

Equipment that processes classified RED information may produce signals capable of unauthorized detection. RED is a term applied to wire lines, components, equipment, and systems that handle national security signals, and to areas in which national security signals occur. BLACK, on the other hand, is a term applied to wire lines, components, equipment, and systems that do not handle national security signals, and to areas in which no national security signals occur.

***TRUSTED SYSTEMS***

***Computers that meet trusting criteria have integrated safeguards into their operation such that only the person "trusted" to have access can actually gain it.***

***Multiple accesses imply the support of multiple simultaneous virtual connections.***

To prevent security compromises of RED information, measures must be taken to reduce sensitive data signals to levels low enough to make detection impossible in areas accessible to unauthorized personnel. These measures include controlled grounding practices which in many cases are in conflict with other subsystem requirements. The recommended approach to grounding a TEMPEST signal reference system is to isolate both RED and BLACK signal/data lines and powerlines. All equipment cabinet grounds, RED signal grounds, and BLACK signal grounds are made with respect to the ground reference established inside the controlled access area (CAA). Both RED and BLACK cable shields are peripherally bonded to equipment cabinets at both ends.

**DoD and NSA Policies Pertaining to AIS Interconnectivity**

Because of the continuing threat to government networks, both externally and internally, interconnection rules and protection measures have evolved. DoD's 5200.28 is the document that provides guidance and direction for the development of security policy by the various defense agencies.

**Applicable Sections from DoDS 5200.28, DoD Trusted Computer System Evaluation Criteria**

DoDD 5200.28 and DCID 1/16 define an AIS as an assembly of computer hardware, firmware and software configured to collect, create, communicate, compute, disseminate, process, store and/or control data or information. An AIS may consist of many computers and peripherals of various sizes that work together in support of a single function. Any computer system that shares

its functionality between the network and other functions (such as administrative word processing) would be identified as an AIS in and of itself.

**Other Related Documents**

In more recent years a large number of new documents related to the Information Assurance (IA) domain have been published describing more detailed information on how to obtain the government's Authority to Operate (ATO). These documents provide information on how to collect the body of evidence acceptable by a Designated Approving Authority (DAA) in order to grant the ATO.