6. INTERNETWORK SECURITY

6.1 Background

a. The SIGNET Designated Network is designed to process data designated up to, and including, "Protected A ... The SIGNET Designated Network will operate in "system-high" mode."[2]

"A system is considered to be operating in the system high mode when all of the following statements are satisfied concerning the users with access to the system, network, its peripherals, remote equipment, or hosts:

- Each user has the appropriate level of personnel screening for all information on the system or network.
- Each user has formal access approval for, and has signed a nondisclosure agreement for all information stored and/or processed on the system or network.
- All users have a need-to-know for some of the information contained within the system or network."

b. The designated LAN will not carry information with a classification greater than Protected A.

c. No connection shall be permitted with external systems unless appropriate safeguards, which have been approved by the departmental security authorities, are in place.

6.2 Implications on SIGNET Internetwork

6.2.1 Local Area Subnetworks

a. The local subnetworks, or LANs, will be physically located wholly within the "system high" operating environment. There are no security requirements which yield security specifications directly impacting the local subnetwork related hardware or software, where local subnetwork connectivity is defined to be provided at the physical layer interface (i.e.. RJ-45 10BaseT jack) in the vicinity of the computing end system and does not include any system related interfaces such as Network Interface Cards.

b. Note that the planned physical / data link layer LAN equipment employs a physical layer broadcast protocol mechanism[2]. The implication is such that all physical layer interfaces into the LAN receive all information transmitted onto the LAN.

c. The physical layer star topology of the planned LAN technology allows operations based policy to limit the threat of unauthorized

[2] Carrier Sense Multiple Access / Collision Detection (CSMA/CD)