STRATEGIC SYSTEMS ARCHITECTURE (SSA)

1. DOCUMENTING SSA GUIDELINES

1.01 SSA APPLICATION GUIDELINES: A new document, The Strategic Systems Architecture (SSA) - Application Developer Guidelines, is currently being developed for 1992/93. It is based on the Strategic Systems Architecture - Application Development Architecture. When completed, a summary will be included in this appendix.

1.02 SSA GOALS: An SSA security goal is that all applications will meet the level of security required by Company policies. The architecture will support a wide range of security levels.

2. SSA ARCHITECTURE

2.01 MODULES: The Architecture views applications to be composed of modules where there is a separation of intended functionality or "concerns." There are three basic categories of modules: The User Interface Modules (UIM), Data Management Modules (DMM) and Process Management Modules (PMM). A combination of these modules interacting with each other in a well defined an consistent manner make up an application.

2.02 REQUIRED SERVICE APPLICATIONS (RSA): The SSA identifies four RSAs: Security Management, Data Repository Management, Address Directory Management, and Systems and Network Management.

2.03 SECURITY MANAGEMENT RSA: The Security Management RSA will provide an application for Security Managers to ensure integrity of application modules, systems, network components, and data.

concerned that the underlying DoD policy is not cost-effective or appropriate for commercial environments. Currently, Bellcore is developing working with government and industry to develop a new document, Minimum Security Functional Requirements (MSFR), which will replace the Orange Book.

2.02 CLASSIFYING RESOURCES: The fundamental aspect of the DoD policy is the security classification of people and documents. One of a hierarchical set of classifications consisting of "unclassified", "confidential", "secret", and "top secret" is assigned to every document. In the case of a computer system, each unique resource is labeled (however, since an interpretation of the Orange Book criteria for database systems has not yet been published, it is unclear whether this labeling would be extended to all fields, tuples, or entries in a database).

2.03 RULES TO PERMIT ACCESS: System users ***MAY*** have access to system resources ONLY if their security clearance, which is also one of the above classifications, is equal to or higher than the classification of the document. In the case of a computer system, each user must receive a clearance. This classification of all data and users would result in considerable cost and Bellcore does not feel it is needed by their clients (this policy is reflected in the B-level Mandatory Access Control mechanisms mentioned above).

2.04 FORMAL SPECIFICATIONS AND ANALYSIS: The formal specification and analysis of security policies (see B and A Groups) also may not be cost-effective in providing additional security for Bellcore's clients.

2.05 COMPARING BUSINESS TO GOVERNMENT: It has been suggested that government and business have different motivating requirements, different inherent risks, and therefore different security needs. The government is most concerned with preventing state secrets from falling into enemy hands. The cost of protecting such information does not really enter into the decision of how much protection to provide. On the other hand, businesses are more profit oriented. Information needs to be protected only to the extent that it is cost-effective to do so.