

~~SECRET~~

IHSA 82-017

7 April 1982

MEMORANDUM FOR:



/ISSG

25X1

FROM:

DDA/IHSA

SUBJECT:

ADP Systems Security - Problem Statement


## Statement of Problem

Developing a comprehensive ADP systems security program for the Agency extends beyond the promulgation of policy & establishment of procedures. Assuming that physical, personal and technical security standards will remain stringent and high, the problem in ADP systems security is one of definition and application. Management must support the policies, the providers must select and apply the controls and the users must understand and operate within the guidelines.

The security threat is real. As more information becomes available at increased data rates to increasing numbers of people, the potential for unauthorized disclosure, accidental loss or destruction, intentional penetration or alteration of data increases proportionally. In formulating a program for computer security these vulnerabilities must not only be identified but countermeasures developed as well as verified. Confidence in the computer systems must be assured. Coupled to the above is the desire to provide a homogeneous environment for Information Handling Systems while maintaining compartmentation and need to know principles.

As concluded by the IHSA Working Group on Information Protection and Management, there is a gap between existing ADP policy and procedures and the current operating environment. The goals developed by this group are indicative of the current perception in that users do not feel comfortable in their knowledge or interpretation of security concerns in ADP systems. These goals are tabulated below:

Goal: Continue emphasis in promulgating security policy and guidelines which more precisely define areas of responsibilities, assign accountability, identify authority and encourage judicious application of technology for the protection of information in the future IH environment.

Objective 1.1: Accelerate the coordination and implementation of DCID 1/16 and  as modified.

25X1

25X1

~~SECRET~~

- Objective 1.2: Provide an acceptable and reliable emergency destruction technique for digitally stored data.
- Objective 1.3: Identify new devices, techniques or methodologies for application in dissemination controls, access limitations, compartmentation, communications security, emanations control and emanation analysis.
- Objective 1.4: Incorporate security enhancements into system design and procurement which will accomplish security policy, for audit trails in particular.
- Objective 1.5: Conduct research in the design and development of reliable, secure information systems, addressing hardware as well as software aspects of information system technology.
- Objective 1.6: Develop acceptable and reliable COMSEC techniques for information protection through the encryption of data bases.
- Objective 1.7: Investigate expansion of current security policy to specify more frequent reinvestigations for selected ADP personnel.

In the IHSA paper presented to EXCOM, the goals for the 1985-1989 timeframe were extrapolated from the above and focused primarily on compartmentation controls, the possible use of secure operating systems, encryption of data bases and TEMPEST protection.

Analysis of the goals and objectives articulated by the Working Group and the extension of those goals by the IHSA provide a perspective on what a cross-sectional representation of the Agency population perceives as weaknesses in our security profile and what needs to be done. It can be deduced, although not empirically, that accomplishment of the objectives stated by the Working Group in the 1982-85 timeframe would be extremely supportive of the IHSA expectations for the 1985-1989 timeframe.

The problem then not only lies in the definition but in achieving a proper balance between apathy and paranoia. A pragmatic approach which does not constrain operational flexibility and efficiency but provides confidence in data integrity, availability and confidentiality is required. Provision of the right information to the right people at the right time remains a basic objective.

From a systems architecture planning perspective, an ADP systems security program requires three major ingredients: These are policy, specification and validation. More specifically there is a need for:

SECRET

~~SECRET~~

- o Specific policy provisions for computer networking
  - Connection of terminals at overseas locations to headquarters computers
  - End-to-end encryption
- o Development of security models as a means of specifying security requirements
- o Policy and practices on validation of systems and networks



25X1

~~SECRET~~