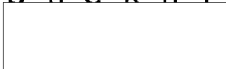


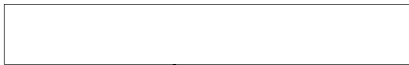
S E C R E T



25X1

22 January 1982

MEMORANDUM FOR:



Information Handling Systems Architect

25X1

FROM:




Chairman, Information Protection and Management Working Group

25X1

SUBJECT:

Report of Working Group V

The final report of Working Group V on Information Protection and Management is attached. Our thanks go to  of your staff, who has ably summarized the results of two full days of meetings and has thoroughly coordinated this paper with working group members.

25X1



25X1

Attachment:

Report of Working Group V

Unclassified when separated from attachment.



25X1

SECRET

Working Group V

25X1

Information Protection & Management

1. Summary and Conclusions
2. Security
 - a. Policy
 - b. Technology Impact
 - c. Disks and Terminal Management
 - d. Personnel and Physical Security Standards
 - e. Dissemination Control and Compartmentation
 - f. Other Security Issues
 - g. Security Goals and Objectives
3. Information Management
 - a. Records Management
 - b. Administration
 - c. Control, Storage and Archiving
 - d. Data Definition Standards
 - e. Goals and Objectives

SECRET

25X1

SECRET

25X1

1. Summary and Conclusions

IHSA Working Group V met on 23 and 24 November 1981 to review the IHSA point paper on Information Protection and Management and discuss other issues relevant to this general area of interest. The objective of these two sessions was to collectively determine and propose the direction the Agency should pursue in the formulation of Security and Information Management strategic goals for the 1985-1989 timeframe. The Group concluded that there is a definite need for 1) establishment of unambiguous security policy concerning Information Handling Systems, 2) judicious selection and attention to technological advances and their application to security safeguards and 3) generating authoritative directives for records management procedures. Based on these holistic conclusions, the group opined that a framework existed from which achievable goals could be formulated to focus IHSA efforts in Strategic Planning.

2. Security

a. Policy

DCID 1/16 and [] provide existing security guidelines and policy regarding ADP systems. Following an explanation of security policy by the OS/ISSG representative, the Working Group agreed that these policies and guidelines do not adequately cover or reflect the current ADP environment nor will they be applicable in the 1985-1989 timeframe. The dynamics involved in Information Handling systems make it difficult for users to find comfort in their adherence to current security policy and guidelines. It was recommended that security policy be promulgated which better defines the aspects of IHS's, and that more explicit responsibilities for adherence to security practices and procedures be established. A rewrite of HR 10-26 and DCID 1/16 is specifically recommended to incorporate current and future policies regarding security. Moreover, security policy should be a major consideration in new system design and development.

25X1

b. Technology Impact

Technology is developing and becoming available which has potential for enhancing ADP system security. This is especially true in the areas of Communications Security, automated dissemination controls to aid in maintaining compartmentation, secure operating systems, and encryption of data bases. Extension of large data bases, such as those envisioned in SAFE, to NFIB membership must incorporate protective measures against the unauthorized or accidental disclosure of sensitive, compartmented information. Connectivity to and interoperability with the Intelligence Community must have multi-level security safeguards.

It was also recommended that reliability requirements for IHS hardware and software be developed to include exhaustive Single Failure Analysis and Security Fault Analysis documentation. As U.S. Government procurements represent only approximately ten percent of the computer market, these specifications, may, in many cases, be difficult to comply with. However, this is considered more cost-effective than to retrofit available commercial hardware with security safeguards.

25X1

Page Denied

Next 9 Page(s) In Document Denied