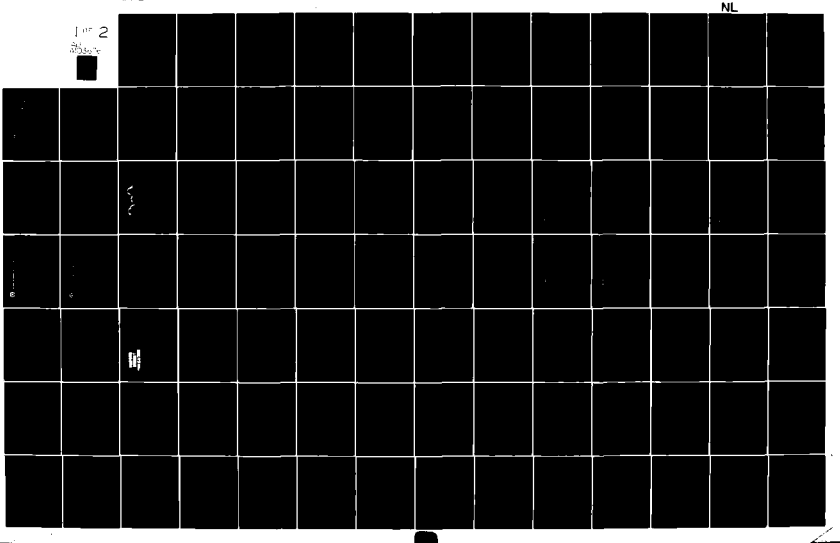
AD-A103 676 OFFICE OF THE SECRETARY OF DEFENSE WASHINGTON DC F/G 9/2
SURVEY OF FEDERAL COMPUTER SECURITY POLICIES.(U)
NOV 80 E V EPPERLY

UNCLASSIFIED NL

1 OF 2



SURVEY OF FEDERAL COMPUTER SECURITY POLICIES

Report of the Policy Survey Subcommittee

November 1980

FOREWORD

This report involved the active participation of the Policy Survey Subcommittee members listed below:

Mr. Stephen F. Barnett
National Security Agency

Mr. Frank M. McClelland
National Communications Systems

LTJG Sharron K. Crowder
Department of the Navy

Mr. Ronald C. Kriston
Central Intelligence Agency

Mrs. Phoebe G. Harper
Defense Intelligence Agency

LtCol Lawrence A. Noble
Department of the Air Force

Mr. Gary E. Johnson
Department of Treasury

Mr. James E. Studer
Department of the Army

Mr. Eugene V. Epperly
Office of the Secretary of Defense
Chairman

It is emphasized that the views and observations contained in this report represent the independent and individual views of the participants, not necessarily the official views of their organizations.

A report such as this must initially be written by one person, and the original version was drafted by the Chairman. This was then circulated to Subcommittee members for critique, modification, and amendments. Although there may remain some disagreement on minor points, the Subcommittee members concur with the final version of the report.

EXECUTIVE SUMMARY

Purpose

This report documents the subcommittee's survey of current Government computer security policy documents at the national and Federal department/agency levels. The review was undertaken to identify what policy exists, what it addresses, and what responsibilities are assigned.

Approach

The following criteria were established for "computer security policy" documents:

1. They must be authoritative and directive in nature;

2. They must reflect in content the multi-disciplinary, total systems approach axiomatic in current computer security policy.

Total coverage of Executive Branch agencies and departments (over 70) was deemed impractical - the effort focused on fifteen agencies that represented over 88% of the Government ADP systems reflected in the GSA inventory and included the majority of Cabinet-level departments.

A questionnaire format was developed to extract on a common basis key attributes of document policy coverage, and this was to be completed by subcommittee members in the interests of reliability and consistency. A key objective of the process was to identify national level policies and authorities. Existence of policy/program oversight mechanisms was identified as a secondary but very important focus. (Section I, pp. 1-5).

Department/Agency Policies

For the fifteen agencies surveyed, 32 separate computer security policy documents (totalling 1,316 pages) were obtained and reviewed. These were consolidated into 27 policy sets of like scope and applicability. All fifteen agencies have promulgated computer security policies; however, these varied in approach, scope and applicability. Survey results reflected the historical sequence of attention to computer security; 63% of the sets reflected policies implementing national security information protection requirements. Other frequencies cited among the 27 policy sets were: Privacy Act, 41%; Transmittal Memorandum No. 1 to OMB Circular A-71, 30%; Intelligence Special Access Programs, 30%; National COMSEC Directive, 15%; OMB Circular A-108, 11%; and, Atomic Energy Act, 7%. Computer security subdisciplines' frequency were reflected in the sets as follows: Physical security, 100%; personnel security, 96%, administrative/procedural security, 96%; hardware/software security, 96%; communications security, 89%; and, emanations security, 70%. (Section II, pp. 6-9)

"National" Level

A most important facet of the survey was to identify higher level authoritative bases for computer security policies at the department/agency level. Thirteen documents forming 5 policy sets were identified and reviewed. As an

operational complement to policy, various program oversight mechanisms were also identified, to include the Legislative Branch.

Comprehensive computer security policy, promulgated by the Office of Management and Budget* and supplemented by further issuances from the Office of Personnel Management (OPM), the General Services Administration (GSA), and the National Bureau of Standards, Department of Commerce (NBS), was revealed. This policy (summarized on pp. 12-14) included:

-- All Federal data and applications processed by computer systems

-- Personal, proprietary, and other sensitive data, to include national security data.

-- Such data and applications processed by other systems on behalf of Federal departments and agencies, as well as by Federal computer systems as such.

Supplementing policies in response to OMB tasking include the following:

-- OPM has amended the Federal Personnel Manual

-- GSA has amended the Federal Property Management Regulations and the Federal Procurement Regulations

-- NBS has issued numerous guideline publications and maintains an ongoing program for standards development.

Other national level policies of narrower scope and applicability included implementation of classified information safeguarding requirements (e.g., NATO, Intelligence, and Atomic Energy-related information) and of requirements for personal information subject to the Privacy Act (Section III, pp. 10-14).

Oversight

A significant amount of national interest in the oversight of Federal computer security activities is identified (e.g., Senate Committee on Government Operations, GAO, the President's Initiative on Fraud and Waste, Information Security Oversight Office, OMB).

Collectively, these have revealed significant problems in the field implementation of computer security policy, particularly systems not processing classified information (Section IV., pp. 15-20; see also Appendix I.).

*Transmittal Memorandum No. 1 to OMB Circular A-71, Office of Management and Budget, "Security of Federal Automated Information Systems," July 27, 1978.

A Federal Agency Perspective

A section describing the context and flow of computer security policies from higher levels is included to illustrate, in an agency organizational context, policy and oversight approaches taken and possible problems with regard to effective implementation of current and future computer security policy requirements. (Section V, pp. 21-25).

Conclusions and Recommendations (Section VI, pp. 26-29)

GAO noted that TM 1 to OMB Circular A-71 "...requires action by top agency managers which could contribute greatly to correcting many of the computer data security problems...it sets an appropriate framework for agencies' initiatives to correct the data security problem."

However, the Subcommittee observed policy fragmentation across-the-board and lack of cost effective, feasible implementing guidance.

The foregoing indicates that a deeper level of analysis is required to focus on those aspects of computer security field implementation that are susceptible to benefit from national level attention and effort. Accordingly, the Subcommittee strongly and unanimously recommends attention be given to the following specific problem areas related to current computer security policies and field implementation thereof:

1. The GAO identified lack of top management support in Federal Departments and Agencies (Appendix I), to specifically include the need for the education and awareness of top management;

2. Closely interrelated, the lack of resources, both research and development resources and operational resources, with specific attention to the problem of trained manpower and funding stability.

3. The problemmatic nature of the hardware/software computer security subdiscipline, to specifically include the development of secure systems technology, security technical evaluation methodologies, and recommended management and operational mechanism(s) therefor;

4. Manifest requirements for means of more effective integration and coordination of identified national policy promulgating activities; and,

5. Generation of feasible and cost-effective implementing guidance for various computer security subdisciplines associated with the implementation of overall computer security policies.

CONTENTS

I. INTRODUCTION

Purpose

The purpose of this report is to document the survey of identified national level and Executive Branch department and agency computer security policies as undertaken by the Policy Survey Subcommittee.

Tasking. The subcommittee was asked to review current government computer security policies at both the national and department/agency levels. The purpose of the review is to identify what policy exists, what it addresses, and what responsibilities are assigned. The task, approach and objectives as refined by the subcommittee are summarized in Figure 1.

Approach and Methodology

Target "Universe." The survey "universe" was initially defined as the major organizational elements of the Executive Branch. The United States Government Manual, the official handbook of the Federal Government published by the General Services Administration (GSA), lists over 70 Executive departments, agencies and other establishments below the level of the Executive Office of the President. Total coverage was not deemed a practical objective.

In view of time and resouce limitations, it was decided to limit the survey of Executive Branch departments and agencies and to concurrently maximize survey coverage by focusing on those entities operating the overwhelming preponderance of government ADP systems, as reflected in the GSA Automatic Data Processing Equipment Inventory In The United States Government, April 1979 edition. In view of their relative importance, it was also decided to include all Executive Departments included in the Cabinet, regardless of the number of computer systems each. (Even though HEW was disestablished as such, it was considered one Executive Department for purposes of the survey, in view of the recency of that action.) CIA, DIA, and NSA were added since their assigned computer security policy responsibilities transcended their immediate organizations, and the Military Departments were included separately by virtue of the comparative size of the organizations and their associated ADP programs. Basically, then, the survey initially was to include 26 Executive departments and agencies, with these organizations accounting for 9257 computer systems out of the GSA total of 9299, or a coverage percentage of 99.5%.

Subsequent further limitations on time and other resources led to the reduction of this "sample universe" to fifteen departments and agencies (Figure 2), thereby covering 8237 ADP systems in the GSA inventory, or over 88.6% thereof, not including CIA or NSA ADP systems, and including seven of the twelve Cabinet-level departments.

Survey Focus. Given the task of surveying computer security policies, the subcommittee focused on computer security documents as such. Rather than include all policy documents mentioning computer security, it was agreed that documents to be reviewed for this survey must meet the following criteria:

POLICY SURVEY SUBCOMMITTEE

TASK: REVIEW FEDERAL GOVERNMENT COMPUTER SECURITY POLICIES
- TO IDENTIFY EXISTING POLICIES, SCOPE, APPLICABILITY & RESPONSIBILITIES
- AT NATIONAL & DEPARTMENTAL LEVELS
- CLASSIFIED AND UNCLASSIFIED INFORMATION

APPROACH: QUESTIONNAIRE SURVEY OF SELECTED NATIONAL & EXECUTIVE BRANCH DEPARTMENT/AGENCY COMPUTER SECURITY DOCUMENTS
- DOCUMENTS ADDRESS COMPUTER SECURITY IN A COMPREHENSIVE SENSE
- QUESTIONNAIRE DESIGNED TO EXTRACT KEY PROGRAM INDICATORS
- DEFINITION OF "SAMPLE" UNIVERSE TO FOCUS ON PREPONDERANCE OF ADPE & CABINET-LEVEL DEPARTMENTS

COVERAGE OBJECTIVES:

1. POLICIES
   -- NATIONAL LEVEL
   -- EXECUTIVE DEPARTMENT/AGENCY LEVEL
2. PROGRAM OVERSIGHT MECHANISMS (SECONDARY)
   -- NATIONAL LEVEL
   -- DEPARTMENTAL/AGENCY LEVEL

Figure 1

SURVEY FOCUS — — EXECUTIVE BRANCH DEPARTMENTS & AGENCIES
GSA AUTOMATIC DATA PROCESSING EQUIPMENT INVENTORY

EXECUTIVE DEPARTMENT/AGENCY	NUMBER OF ADP SYSTEMS	CUMULATIVE % OF TOTAL
ARMY	1126	
NAVY	1473	
AIR FORCE	1704	
● DEFENSE	4535	49%
● ENERGY	2395	75
NASA	489	80
● TRANSPORTATION	371	84
● TREASURY	174	
● HEW*	137	
● AGRICULTURE	102	
● JUSTICE	33	
NRC	1	88.6
DIA	(INCLUDED IN DOD TOTAL)	
CIA	(NOT INDICATED IN INVENTORY)	
NSA	(NOT INDICATED IN INVENTORY)	
	8237 (OUT OF 9299)	

●– CABINET LEVEL DEPARTMENTS

*– CONSIDERED ONE DEPARTMENT FOR SURVEY PURPOSES

Figure 2

1. They must reflect in content the overall multidisciplinary, total systems approach that has emerged as axiomatic in computer security policy and practice, to include explicitly the preponderance of the necessary subdisciplines that in aggregate represent the accepted approach to securing computer systems in operational environments, as suggested in Figure 3.

This criterion includes documents that in themselves do not contain all such subdisciplinary requirements, but explicitly reference such requirements for implementation, where these requirements are promulgated in other documents (e.g., DoD Directive 5200.28 and associated ADP Security Manual [1,2] explicitly refer to and require implementation of communications security and emanations security requirements promulgated generically by separate DoD Directives on those subjects).

Not to be included were documents that treated in separate and stand-alone fashion various facets or aspects of computer system security (e.g., Defense's Information Security Program Regulation, DoD 5200.1-R [4], which for ADPE includes only security marking provisions for certain ADP media).

2. They must be directive in nature, authoritatively imposing computer security responsibilities and requirements of a designated scope and applicability.

Excluded by this test were documents such as National COMSEC/EM SEC Information Memorandum No. 7002, "COMSEC Guidance for ADP Systems" [5], which contains computer security guidelines. Similarly excluded were a host of published National Bureau of Standards guidelines, many of which are enumerated at Appendix A [6].

Questionnaire Coverage and Scope. The approach decided by the subcommittee involved development of a questionnaire format to be used in reviewing and extracting relevant information from current computer security policy documents meeting the above criteria. The format (attached as Appendix B with associated guidance, and summarized in Figure 4) was designed to extract on a common basis key attributes and aspects of department/ agency policy document coverage. The completed questionnaire would provide a policy/program profile for each computer security policy document (or document set, as noted below), and questionnaires cumulatively considered would provide a fairly accurate general indicator of computer security policy coverage both at the Executive department and agency level and at the Executive Branch level.

A key derivative objective of the department/agency survey was to identify other potential national-level computer security policies in policy documents not already identified in the questionnaire or otherwise obtained (i.e., Question #3, "authoritative basis(es) for policy"). This aspect is deemed critical to the overall issue concerning the extent to which policy computer security policy exists at the national (essentially meaning Executive Branch) level of the Federal Government.

The first three items on the questionnaire ("Identification" and "Authoritative Bases" on Figure 4) are followed by items on applicability and scope. These are considered essentially self-explanatory indicators where presence or

COMPUTER SECURITY

AN INTEGRATED, MULTI-DISCIPLINARY APPROACH IS REQUIRED

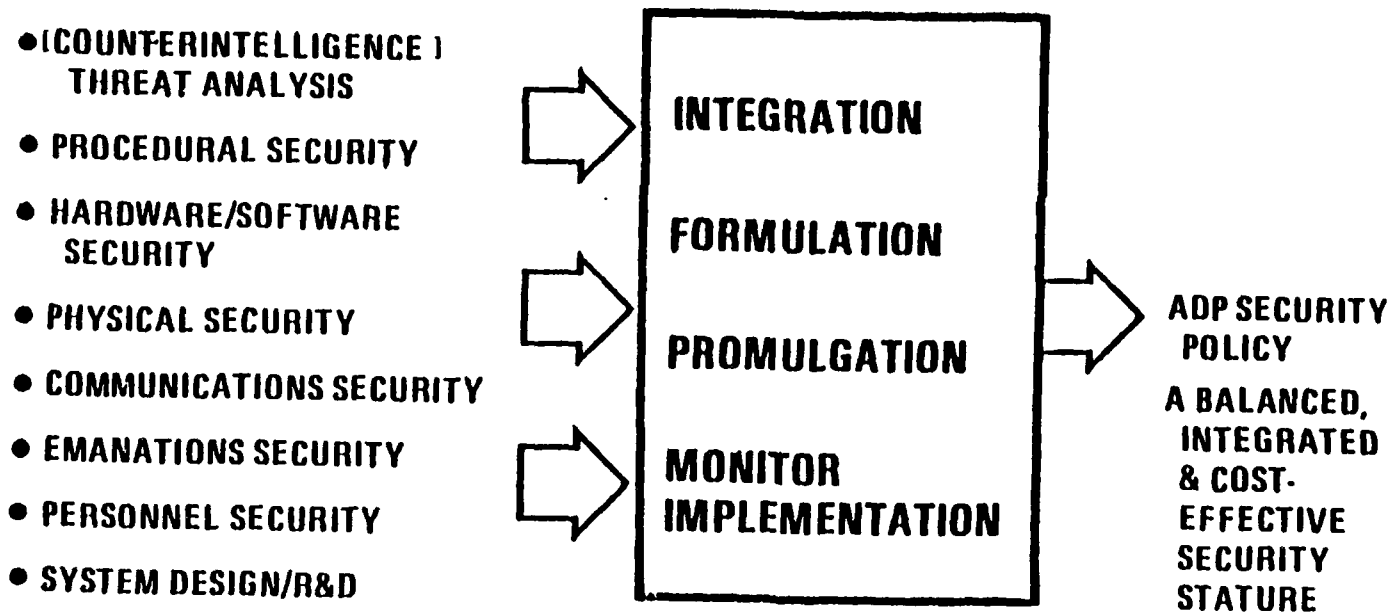


Figure 3

QUESTIONNAIRE COVERAGE

- OBJECTIVES: - IDENTIFY EXISTING POLICY SOURCES AT THE NATIONAL LEVEL
  - DESCRIBE GENERAL NATURE AND SCOPE OF IMPLEMENTATION AT DEPARTMENT/AGENCY LEVEL

- QUESTIONNAIRE SCOPE:
  - SOURCE & DOCUMENT(S) IDENTIFICATION
  - AUTHORITATIVE BASES
  - APPLICABILITY ("IN-HOUSE" AND/OR "OUT-HOUSE")
  - PROTECTION SCOPE
    - -- INFORMATION/DATA
    - -- SYSTEMS/AREAS/SOFTWARE/ OTHER SYSTEMS RESOURCES
    - -- LIFE CYCLE COVERAGE? (ADP SYSTEMS AND/OR DATA SYSTEMS)
  - SUBDISCIPLINES INCLUDED
    - -- PERSONNEL SECURITY
    - -- PHYSICAL SECURITY
    - -- COMMUNICATIONS SECURITY
    - -- EMANATIONS SECURITY
    - -- ADMINISTRATIVE/PROCEDURAL SECURITY
    - -- HARDWARE/SOFTWARE SECURITY

Figure 4

QUESTIONNAIRE COVERAGE (CONT'D)

- PROGRAM COMPONENT ELEMENTS:
  - -- ASSIGNMENT OF RESPONSIBILITY
  - -- MANAGEMENT CONTROL PROCESS
  - -- DESIGNATED APPROVING AUTHORITIES
  - -- OVERALL SECURITY SPECIFICATIONS/REQUIREMENTS
  - -- SECURITY EVALUATION REQUIRED FOR SYSTEM OPERATION
  - -- AUDIT OR OTHER FOLLOW-UP SECURITY EVALUATION
  - -- RISK ANALYSIS METHODOLOGIES
  - -- SECURITY REQUIREMENTS FOR PROCUREMENT
  - -- REQUIREMENTS FOR CONTINGENCY PLANNING
  - -- PERSONNEL SCREENING
  - -- SPECIFIED WAIVER AUTHORITY
  - -- REQUIREMENT FOR ADP SECURITY BUDGET
- NUMBER OF ADP SYSTEMS COVERED
- NUMBER OF PAGES

Figure 4 (Cont'd)

absence can be considered coverage attributes for a given policy document/ computer security program. Similarly straight forward are the subdiciplines included (item 6 on the questionnaire at Appendix B). The last substantive item, "Program Component Elements," #7 on the questionnaire, is an adoption of the checklist developed to review department and agency implementation plans for the requirements imposed by Transmittal Memorandum No. 1 to OMB Circular A-71, "Security of Federal Automated Information System" [7], the most comprehensive computer security policy document identified herein in terms of organizations levels, scope, applicability and system security coverage. Accordingly, this item in particular was designed to reveal gaps in program policies.

Questionnaire Completion. In the interest of maximizing response consistency and reliability, documents were reviewed and questionnaires were completed only by members of the subcommittee. In furtherance of that goal, interpretive guidance was also developed and provided (included in Appendix B) prior to completion of the questionnaires.

Limitations. The following limitations in survey scope, methodology and coverage are specifically noted for the reader. First of all, the survey represented neither a random nor a representative sample. In view of limitations in time and resources, focus was upon coverage of those agencies representing the preponderance of government computer systems as reflected in the GSA inventory. The objective was not only to indicate policy per se, but to suggest relative degree of coverage within the Executive Branch in terms of number of systems included. Additionally, documents obtained by the subcommittee came from personal contacts of the subcommittee members and from subcommittee members' files. Specific agency coverage is noted herein. However, while coverage is considered extensive by virtue of members' collective experience in this field, there may be other national level documents not here included.

Further, although inference may be made concerning overall relative quality of documents in terms of indicators specified, the subcommittee did not attempt to directly address evaluation of national or department/agency computer security policy and associated programs. The primary consideration for survey purposes was to identify presence or absence of the particular policy attribute, not even relative degree of completeness. For example, on question 7a(1) of the questionnaire, a policy document may assign program responsibility poorly (e.g., fragmented assignment to multiple organizational elements, with no one element having overall responsibility), but the document does assign computer security program responsibilities.

A second very important follow-on facet of an effective security program is the nature and extent of program oversight. An attempt was made in this survey to indicate these mechanisms where they are known to exist; however, coverage thereof is incomplete. Since some oversight activities have clearly indicated negative findings, promulgating sound policy is often just the first step in obtaining effective field implementation.

Other aspects viewed as critical to the effective implementation of government computer security programs are not directly addressed in this survey. Included here are the relative degrees of higher level management support, and often correlated therewith, relative allocation of resources,

both manpower and funding. A relative measure of management support may be inferred from the existence per se of both department/agency and national level policies and from established oversight mechanisms; however, comparative evaluation of computer security field implementation is clearly beyond the scope of this report.

Report Organization. The following sections reflect, in sequence: results of the survey of Executive Branch department and agency computer security policy documents; similar treatment of policy documents identified at the national/Executive Branch level; description of such oversight mechanisms as exist at the national level and have to varying degrees concerned themselves with computer security as such, or in the case of the Information Oversight Office, manifest the intention and probable potential to do so; and a description of higher-lever policies' impact on one organization at the department/agency level.

Terminology

For purposes of this report, the following definitions are employed.

First of all, a policy is simply considered a decision made in advance and independent of a specific instance or particular situation, which is promulgated in an authoritative, directive issuance. A security policy is such a decision that essentially contains the following elements:

1. Some asset or assets deemed to be of value

2. Some perceived threat or set of threats to the asset(s)

3. Some vulnerability or vulnerabilities associated with the asset(s)

4. A resultant risk scenario incorporating the foregoing, and

5. A decision concerning the relative allocation of protection resources.

Computer security policies involve computer systems and the associated information processed and/or functions performed as the assets to be protected.

The terms, "computer system", "computers" and "ADP system" as used herein apply to "Automatic Data Processing Equipment" as defined in the Automatic Data Processing Equipment Inventory in the United States Government, published by the General Services Administration (GSA) [8], to specifically include associated equipment* (i.e., computers plus auxiliary and accessorial equipment), facilities, personnel, software, data and procedures.

*Recent General Services Administration commodity decisions have resulted in the reclassification of the majority of word processing equipment into Federal Supply Classification Group 70, "General Purpose Automatic Data Processing Equipment." Some computer security policy documents have begun to include word processing systems and equipment (e.g., [13]).

"Agency" is here used as in 5 U.S.C. 522(e), meaning any executive department, military department, Government corporation, Government-controlled corporation or other establishment in the Executive Branch of the Government (including the Executive Office of the President or any independent regulatory agency) [9].

"Classified information" means information and material determined to require protection against unauthorized disclosure in the interest of national security (i.e., the national defense and foreign relations of the United States) and designated a level of classification pursuant to Executive Order 12065[10] or prior order, or classified as provided in the Atomic Energy Act of 1954, as amended.

II. EXECUTIVE BRANCH DEPARTMENT AND AGENCY POLICIES

As noted, the documents reviewed for this survey were limited to only those that authoritatively treated computer security in an essentially wholistic sense (i.e., overall focus on computer systems and/or automated data and applications, as well as inclusion of the multiple computer security subdisciplines noted above). This has included both documents specifically on computer security (e.g., DoD Directive 5200.28 [1]) as well as sections or parts of larger documents that meet the previously stated criteria as essentially comprehensive computer security documents in themselves (e.g., Part 6 on computer security, which is a section of HEW's ADP Systems Manual [11], or Agriculture's "ADP Security and Privacy" chapter of their "Departmental Information Processing Standards Manual" [12]).

The following tabulated results, which are derived from survey of the cited Executive Branch Agencies and Departments, involved the review of 32 separate documents (listed in Appendix C). However, in some cases more than one document constituted a single policy set of the same scope and applicability. In such cases, one questionnaire was completed for both documents. An example is DoD Directive 5200.28 and its companion, amplifying ADP security manual, DoD Manual 5200.28-M. Accordingly, the Department/Agency "data base" of questionnaires consists of 27 questionnaires, reflecting 32 documents reviewed. All of these were formally promulgated policies, except for one proposed draft, and they totaled 1,316 pages.

Results

A summary questionnaire, reflecting both numerical, cumulative positive responses, as well as respective percentages thereof from the total number of department/agency questionnaires, is attached as Appendix D.

Authoritative Bases. Sixty-three percent of the questionnaires reflected policies in implementation of national security information protection responsibilities assigned by Executive Order 12065. Additional authoritative bases associated with national security information and the percentage of positive responses are the following:

Atomic Energy Act of 1954, 7%
Special Access Programs for Intelligence (E.O. 12036, DCID No. 1/16), 30%
E.O. 10865, "Safeguarding Classified Information within Industry", 15%
E.O. 12036 as such, 7%
National Communication Security Directive, 15%

Authority for unclassified information included the following:
Privacy Act of 1974, 41%
The related OMB Circular A-108, 11%
Transmittal Memo #1 to OMB Circular A-71, 30%
Records exempt from disclosure under the Freedom of Information Act, 7%

Others noted with only one positive response are identified in the summary questionnaire (Appendix D).

Applicability. Twenty-five of the questionnaries, or 93%, reflected documents applying to the originating department of agency and its components and facilities. Twenty-three, or 85%, further applied in some fashion to department/agency contractors. (NOTE: Many of these agencies participated in the Defense Industrial Security Program which covers all contractors handling classified information except when the ADP systems are agency owned and controlled and are located on agency premises, but contractor operated -- in this case, the agency vice the Industrial Security Manual [13] may prescribe required security measures).

Scope. For information/data included within the policy documents positive responses were the following:

Classified National Security Information, 78%
Unclassified "National Security Related Information", 30%
Personal Information Related to Individuals ("Privacy"), 59%
Other agency/department "Sensitive Information and Records", 52%

Other attributes of policy scope included the following:

ADP systems (i.e., "Automatic Data Processing Equipment", including computers and auxiliary or accessorial equipment such as I/O devices and communications equipment), 100%
Areas housing ADP systems and their components, 82%
Computer Programs (i.e., software), 89%
Other ADP resources and supplies, 63%

Responses concerning policies that generally contained security requirements pertaining to the entire life cycle were as follows:

ADP or computer systems specified, 85%
Individual data/application systems, 63%

Computer Security Subdisciplines. Responses here include requirements that may be enumerated in a separate document but are specifically cited as policy requirements; for example, the computer security policy document requires personnel security or communication security actions set forth in a referenced, separate document. Results are as follows:

Personnel security, 96%
Physicial Security, 100%
Communications security, 89%
Emanations security, 70%
Administrative/Procedural security, 96%
Hardware/software security, 96%

Program Component Elements. Positive questionnaire responses concerning various elements of agency/department computer security policies and associated programs are as follows:

a. Assignment of Responsibility:

(1) For computer security within the Agency or Department (i.e. specification of a headquarters staff element as responsible for policy promulgation and program oversight), 96%

(2) For specific ADP systems or ADP installations (e.g. Appointment of ADP System Security Officers), 93%

b. Management Control Process to assure that administrative, physical, technical and other safeguards are included in agency computer systems; 96%

c. Formally designated approving authority for the security aspects of covered ADP systems; 78%

d. Overall security specifications/requirements; 85%

e. Review, test and/or evaluation required as a basis for system approval for operation; 74%

f. Audit or other follow-up system or program security evaluations; 78%

g. Risk Analysis or Risk Assessment methodologies; 70%

h. Security Requirements/Specifications Applicable to Procurement (i.e. equipment, systems or related services); 74%

i. Requirements for Contingency Planning; 67%

j. Personnel Screening Requirements; 78%

k. Specification of an authority to grant waivers; 56%

l. Requirement to specify an ADP security budget; 15%

Summary Comments

Of the fifteen Executive Branch departments and agencies surveyed, all had some computer security policy promulgated. Within that number, however, there are manifest differences in approaches (e.g. one omnibus document or separate documents associated with separate authorities), scope and applicability.

Authoritative Bases as distributed appear to follow the historical sequence of various communities' concern with the subject. The area of classified national security information was the first known to give serious concern, and the first computer security policy documents known emerged here e.g., DoD Directive 5200.28 in 1972. Reflecting that sequence, the greatest number of positive responses (63%) are associated with Executive Order 12065, "National Security Information," [10] the omnibus E.O. charging

protection of classified national security information (this would include E.O. 12065's predecessors). Second most frequently cited authority is the Privacy Act of 1974 (41%) and associated OMB Circular A-108 [9], "Responsibilities for the Maintenance of Records About Individuals by Federal Agencies." Third is the most recent Executive directive in this area, which includes all classified and nonclassified information, Transmittal Memorandum No. 1 to OMB Circular A-71, issued in 1978 [7] (30% positive responses).

It would be expected that this last percentage will increase over time, based on past experience. For example, DoD Component implementing documents for DoD Directive 5200.28 required about two years for development, staffing and review -- this was development of subordinate echelons' policy documents only, not the establishment of effective implementing programs in the field -- and the scope and applicability of DoD Directive 5200.28 is in many aspects substantially narrower than TM 1 to OMB Circular A-71.

III. "NATIONAL"-LEVEL COMPUTER SECURITY POLICIES

Perhaps the most significant facet of the subcommittee's efforts relative to the primary purposes of the parent Computer Security Working Group was a derivative effort, through the survey of departmental and agency policy documents, to identify applicable national issuances meeting the selection criteria set forth earlier. It is also a facet most directly related to the associated NCSC proposal cited initially here. A diverse set of such existing policies were revealed, ranging from some of quite narrow scope to the OMB policy requirements below which are very broad in scope (i.e., all Federal department/agency data and applications processed by computer, to include contractor activities effected on behalf of a department or agency).

National Security Information

Historically, computer security policies first emerged in various functional areas where the handling of classified national security information was involved. As noted in the preceeding department/agency survey results, the most commonly cited authoritative basis for an agency policy (63%) was Executive Order 12065 [10] or its predecessors (e.g., E.O. 11652, 1972; E.O. 10501, 1953, and so on), although none of these Executive Orders qualify as "computer security policy documents" as defined herein. In implementing the basic charge, however, some agencies have developed computer security policy dealing with national security information in the ADP environment and so have authorities for various types of Special Access Program information. The former are covered in the previous section, the latter include the following:

NATO - The Secretary of Defense functions as U.S. Security Authority for NATO Affairs (USSAN), and the U.S. complies with securoty requirements for the protection and handling of NATO classified information by virtue of international treaty.

These are implemented by USSAN Instruction 1-69, "Implementation of NATO Security Procedure (U)," (CONFIDENTIAL), which in turn implements NATO RESTRICED Document C-M(55)15(Final), "Security Within the North Atlantic Treaty Organization," March 8, 1955, as amended. Enclosure "C" to the latter document contains a Section X, "Protection of Classified Information Handled and Stored in Automatic Data Processing Systems" that applies to NATO commands and agencies as well as member nations [15], including the U.S., that use NATO classified information, including ADP systems used solely for communications purposes. Also included therein are special restrictions on the use of U.S. Special Access Program information (i.e., "US SIOP").

Intelligence - The Director of Central Intelligence has promulgated computer security policies for the protection of "intelligence information" (i.e., foreign intelligence and foreign counterintelligence as defined in Section 4, Executive Order 12036, and as classified under the provisions of Executive Order 12065) involving sensitive intelligence sources and methods. The basic Director of Central Intelligence Directive and associated "Computer Security Regulation" set forth computer security policy requirements for ADP systems and networks that process "intelligence information" and apply to both government and contractor ADP systems and networks. Excluded, however, are ADP systems and/or networks that are used exclusively for telecommunications services.

Programs for Government Classified Contracts

Defense Industrial Security Program. By virtue of the number of departments and agencies included and an authoritative basis provided by Executive Order 10865 [16], the Defense Industrial Security Program approaches an Executive Branch-level computer security program.

The Program is administered by the Defense Department on behalf of sixteen other Executive Branch agencies in addition to the DoD components. It is based on a "one face to industry" approach, established under the Executive Order in recognition of the conflicts and lack of uniformity that would result if each agency developed its own industrial security program. Accordingly, the E.O. specifically provided for the extension of the DoD program to include other Federal agencies (Figure 5).

Program policies meet the computer security policy document test herein and are primarily contained in Section XIII of the "Industrial Security Manual for Safeguarding Classified Information," DoD Manual 5220.22-M, April 1980 [13].

The computer security policies included in the program are of relatively long standing (efforts to develop computer security training for DoD Industrial Security inspectors began in 1969), and the most recent addition has been adoption of interim security requirements for word processing systems and equipment (pending formal coordination and final approval).

Other Agency Programs. Of the fifteen agencies reviewed by this survey, all are included within the DISP but Department of Energy, Nuclear Regulatory Commission and the CIA. Each of these have analogous policies and programs for inspection and approval of contractor facilities (e.g., [18 & 19]). There are also similar industrial programs for Special Access Program information, such as DIA's [20].

Personal Information Subject to the Privacy Act

The Privacy Act of 1974 (Public Law No. 93-579, 5 U.S.C. 55a) is implemented within the Executive Branch primarily through Office of Management and Budget (OMB) Circular No. A-108, "Responsibilities for the Maintenance of Records About Individuals by Federal Agencies," as amended [9] (i.e. Transmittal Memorandum No. 5 to OMB Circular A-108, August 3, 1978). The Circular defines responsibilities for implementing the Privacy Act "to assure that personal information about individuals collected by Federal agencies is limited to that which is legally authorized and necessary and is maintained in a manner which precludes unwarranted intrusions upon individual privacy." Relative to this report, the Circular applies to all Federal agencies and requires the head of each agency to "establish reasonable administrative, technical, and physical safeguards" for protecting personal information subject to the Act, to include such information handled by ADPE, and such information handled by government contractors.

Specific tasking associated with the computer environment included the following:

INDUSTRIAL SECURITY PROGRAM ADMINISTRATION

AUTHORITIES:

- EXECUTIVE ORDER 10865
- EXECUTIVE AGREEMENTS BETWEEN THE SECRETARY OF DEFENSE AND:

ADMINISTRATOR, NATIONAL AERONAUTICS & SPACE ADMINISTRATION

SECRETARY OF COMMERCE

ADMINISTRATOR, GENERAL SERVICES ADMINISTRATION

SECRETARY OF STATE

ADMINISTRATOR, SMALL BUSINESS ADMINISTRATION

DIRECTOR, NATIONAL SCIENCE FOUNDATION

SECRETARY OF THE TREASURY

SECRETARY OF TRANSPORTATION

SECRETARY OF THE INTERIOR

SECRETARY OF AGRICULTURE

SECRETARY OF HEALTH, EDUCATION & WELFARE

SECRETARY OF LABOR

ADMINISTRATOR, ENVIRONMENTAL PROTECTION AGENCY

ATTORNEY GENERAL, DEPARTMENT OF JUSTICE

DIRECTOR, U.S. ARMS CONTROL & DISARMAMENT AGENCY

DIRECTOR, FEDERAL EMERGENCY MANAGEMENT AGENCY

PROGRAM "USER AGENCIES" ALSO INCLUDE: THE OFFICE OF THE SECRETARY OF DEFENSE, THE ORGANIZATION OF THE JOINT CHIEFS OF STAFF, THE MILITARY DEPARTMENTS AND THE DEFENSE AGENCIES

Figure 5

-- The Secretary of Commerce was tasked to issue standards and guidelines on computer and data security; and,

-- tne Administrator of General Services was tasked to "revise computer and telecommunications procurement policies to provide that agencies must review all proposed equipment and services procurements to assure compliance with applicable provisions of the Act; e.g., Report on New Systems."

Omnibus Policy -- The OMB Federal Computer Security Program

In announcing establishment of a Federal computer security program (TM 1 to OMB A-71 [7]) in July 1978, OMB Director McIntyre said, "Computer technology now impacts almost every facet of American life. The protection of the technology against unwarranted, unauthorized and illegal uses is a major challenge. This program addresses that challenge in the Federal community" (emphasis added) [21]. The scope, applicability and other attributes of the program are described below.

OMB Computer Security Program Minimum Requirements. The OMB-directed computer security program requires, "at a minimum", each Federal department and agency to:

- Assign responsibility for the security of each computer installation operated by or on behalf of the agency to a management official knowledgeable in data processing and security;

- Establish personnel security policies for all Federal and contractor personnel involved in the design, operation, or maintenance of or having access to data in Federal computer systems;

- Establish a management control process to assure that appropriate administrative, physical and technical safeguards are incorporated into all new computer applications and significant modifications to existing applications (for applications deemed "sensitive," this includes: prior definition and approval of security specifications and the conduct, approval and certification of design reviews and application systems tests);

- Conduct periodic risk analyses for each computer installation operated by or on behalf of the agency (at least every five years);

- Assure that appropriate security requirements are included in the specifications for the acquisition or operation of computer facilities or services (above-cited management official must review, approve and certify the sufficiency of these requirements);

- Conduct independent periodic audits or evaluations and recertify the adequacy of the security safeguards of each operational sensitive application (at least every three years); and,

- Assure that appropriate contingency plans are developed and maintained to provide for continuity of operations should events occur which prevent normal operations; periodically review and test these plans.

OMB Tasking for Additional Requirements. *In support of the program, OMB has further tasked the following agencies as indicated below:

- The Department of Commerce to develop and issue comuter system security standards and guidelines;

- The General Services Administration to issue policies and requlations for the physical security of computer roomd and assure that securoty requirements are included in agency procurements; and,

- The Office of Personnel Management to establish personnel security policies for Federal personnel associated with computer systems.

Supplemental Central Agency Policy

Pursuant to the above OMB tasking, the Office of Personnel Management (OPM) has already promulgated Federal personnel security policies in this area, and the General Services Administration (GSA) has apparently fulfilled their tasking. National Bureau of Standards, Department of Commerce, has published a substantial number of computer security guidelines (Appendix A) and is engaged in standards development efforts.

Office of Personnel Management. On November 14, 1978, OPM issued their Federal Personnel Manual Letter 732-7, "Personnel Security Program for Positions Associated with Federal Computer Systems [22] (subsequently incorporated into the Federal Personnel Manual). Pursuant to responsibilities assigned by TM-1, OMB A-71, the bulletin was the first step in establishing personnel security policies for screening all individuals participating in the design, operation or maintenance of Federal computer systems or having access to data in Federal computer systems, to include both Federal employees and contractor personnel. OPM Bulletin No. 732-2, January 11, 1980 further set forth authorities for investigating contractor personnel and procedures for requesting such investigations from OPM [23].

With regard to Federal employees, the OPM guidance established criteria for designating personnel position sensitivity "to be viewed separately, but in addition to the more traditional relationship to the national security" as currently employed under E.O. 10450 [24].

General Services Administration. GSA actions included amendments to the following documents:

-- Federal Property Management Regulations. Amendments (FPMR Amendment F-42 [25]) have been published in August 1980. The amendment to FPMR Part 101-35* provides government-wide security management guidance for the protec-

*Specifically noted by the Subcommittee is a conflict between provisions of the FPMR part cited and the provisions of Presidential Directive/NSC-24, Subject: "Telecommunications Protection Policy (U)," as revised February 9, 1979, with regard to authority and jurisdiction in the area of telecommunications. Another conflict of authorities from separate policies is identified on page 25.

tion of ADP and telecommunication systems and facilities. This new subpart contains the policy provision that "Federal agencies shall insure that an adequate level of security is provided for all ADP and telecommunication systems and services, including those provided by contractors," and then defines and describes associated requirements and responsibilities. The amendments to subpart 101-36.7, "Environment and Physical Security," provide guidelines to Federal agencies on the environmental and physical security of ADP facilities.

-- Federal Procurement Regulations. Amendments (FPR Amendment 210) [26] published in October 1980 included the following pertinent to computer security:

Section 1-4.1104 added the requirement that agencies' computer security requirements be included in agencies' procurement requests to GSA.

Section 1-4.1107-21 prescribes Government computer security requirements in connection with solicitations, contracts, and contract administration.

Summary Comments

The foregoing demonstrates the existence of Federal computer security policies and associated programs. The most critical one of these, however, is the policies, responsibilities and program established by OMB under the auspices of Executive Branch implementation of portions of the Brooks Act (i.e., OMB Circular A-71 as such):

> "This includes responsibility for the establishment of physical, administrative and technical safeguards required to adequately protect personal, proprietary and other sensitive data not subject to national security regulations, as well as national security data" (emphasis added) (Paragraph 4., [7]).

The requirement to effectively integrate numerous relatively independent programs becomes even more manifest when one considers the contractor arena in conjunction with the programs enumerated above. The Industrial Security Program alone precludes industry from having to deal with seventeen or more separate programs in the classified arena. Industry has expressed concern with this happening in implementation of TM-1 to A-71, and the same concern with regard first to OPM policies implementing TM-1 prompted the Assistant Secretary of Defense (Comptroller) to suggest to OMB that implementation of the contractor employee personnel security requirements of TM-1 be carried out by means of a modification of the existing Industrial Security Program, to coordinate and effect uniform implementation. The same rationale could be said to apply for the further extension of the Industrial Security Program's current nation-wide capabilities for the on-site inspection and approval of contractor ADP systems in the broadest sense.

IV. NATIONAL COMPUTER SECURITY POLICY & PROGRAM OVERSIGHT

As suggested above, promulgation of computer security policy is step one in achieving the end result -- acceptably secure operating computer systems. While the identification of policy/program oversight and monitorship was not an explicit charge of the subcommittee, such activities were duly noted during the course of the survey, along with the manifest fact that these activities often detail clearly negative findings with regard to implementation in the field of already established policy. Accordingly, in at least large, complex organizations, such formal oversight activities are deemed required for essential feedback on policy implementation, particularly as a basis for effecting corrective action.

There follows a summary of oversight activities and related attention to the specific problem of computer security in its various facets -- this summary clearly indicates that concern, including concern transcending the Executive Branch, exists and that computer security policy oversight mechanisms at the Executive Branch/national levels likewise are in place and operating, as a complement to promulgated policy. The sequence of highlighted activities is summarized in Figure 6. However, no attempt is made to evaluate the comparative effectiveness or other attributes of these mechanisms, singly or in combination.

The Congress & The General Accounting Office

Interest in computer security matters by the Congress has stemmed from broader concern for the effective management of computer and information resources (e.g. enactment of the 1965 Brooks Act, P.L. 89-306), and the growing awareness over the past decade of the value and sensitivity of Federal ADP programs and services. The Privacy Act of 1974 (P.L. 93-567) was an early milestone in the 1970's that specified protection of personal data, and since many Federal personnel and other data systems with personal data are automated, the Act led to increased emphasis on the use of computer security measures per se.

1976 GAO Reports. More comprehensive concern for computer security as such was focused by the publication of three reports on facets of computer security in the Spring of 1976 by the General Accounting Office (GAO), an investigative and auditing arm of the Congress. These were "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government," April 23, 1976 [27]; "Computer-Related Crimes in Federal Programs," April 27, 1976 [28]; and, "Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities," May 10, 1976 [29].

Senate Staff Studies. Shortly thereafter, the Chairman of the-then Senate Committee on Government Operations (now Senate Committee on Governmental Affairs), Senator Ribicoff, announced that he had directed the Committee staff to conduct a preliminary inquiry into the problems associated with the areas highlighted by GAO. The Committee subsequently issued two studies dealing with computer security. The first, entitled "Problems Associated with Computer Technology in Federal Programs and Private Industry -- Computer Abuses," [30] reviewed some of the major issues and problems, and it included the three 1976 GAO studies cited above.

NATIONAL LEVEL INTEREST

1976 **GAO REPORTS:**

- "IMPROVEMENTS NEEDED IN MANAGING AUTOMATED DECISIONMAKING BY COMPUTERS THROUGHOUT THE FEDERAL GOVERNMENT" (APR 76)
- "COMPUTER-RELATED CRIMES IN FEDERAL PROGRAMS" (APR 76)
- "MANAGERS NEED TO PROVIDE BETTER PROTECTION FOR FEDERAL AUTOMATIC DATA PROCESSING FACILITIES" (MAY 76)

SENATE COMMITTEE ON GOVERNMENT OPERATIONS:

- "COMPUTER ABUSES--PROBLEMS ASSOCIATED WITH COMPUTER TECHNOLOGY IN FEDERAL PROGRAMS & PRIVATE INDUSTRY" (JUN 76)

1977

- "COMPUTER SECURITY IN FEDERAL PROGRAMS" (FEB 77)

OMB:

- "SECURITY OF FEDERAL AUTOMATED INFORMATION SYSTEMS," TRANSMITTAL NO. 1 TO OMB CIRCULAR NO. A-71

DRAFT FOR COORDINATION (SEP 77)

1978 FINAL ISSUANCE (JUL 78)

PRESIDENT: INITIATIVE TO ATTACK FRAUD & WASTE

- DOD STEERING GROUP ON OVERSIGHT OF DEFENSE ACTIVITIES

SUBCOMMITTEE ON COMPUTER FRAUD

GAO REPORTS:

1979

- "AUTOMATED SYSTEMS SECURITY--FEDERAL AGENCIES SHOULD STRENGTHEN SAFEGUARDS OVER PERSONAL AND OTHER SENSITIVE DATA" (JAN 79)
- GAO LETTER TO SECDEF (MAR 79)

Figure 6

A 1977 follow-up report [31] by the staff included recommendations that the Office of Management and Budget (OMB) direct Federal agencies to put into effect appropriate computer security controls and safeguards and that Federal agencies improve coordination of computer resource protection efforts, develop additional computer security standards and establish personnel security policies. (As noted above, OMB has initiated a computer security program in keeping with these recommendations and the statutory requirements of the Privacy Act of 1974).

Based partly on the foregoing, Senator Ribicoff also introduced the "Federal Computer Systems Protection Act of 1977", S. 1766. With no final action in the 95th Congress, the "Federal Computer Systems Protection Act of 1979" (S. 240; H.R. 6196 in the House) was introduced by Senator Ribicoff. The Bill in essence would make it a crime to use or attempt to use a computer with intent to defraud or obtain property falsely and to embezzle or steal property. On Nov. 6, 1979, the Senate Judiciary Subcommittee on Criminal Laws and Procedures referred an amended version of the Bill to the full Committee for consideration.

More recently, the GAO initiated a Government-wide survey of ADP System Backup Planning in October 1979 (e.g., USGAO letter of September 19, 1979, to Secretary of Defense Brown), keyed among other things to implementation of the relevant provision in TM #1 to OMB Circular A-71.

Office of Management and Budget, Executive Office of the President

OMB has formally promulgated omnibus, comprehensive computer security requirements for Federal government data and applications processed by government or contractor computer systems in July 1978 [7]. The promulgating document called for each Executive Branch department and agency to provide OMB with an implementation plan. To oversee program implementation and specifically review department/agency implementation plans, OMB initially established an ad hoc team in December 1978. Due to the wide variance in the nature and organization of department/agency implementation plans, the team developed the OMB checklist for purposes of more consistent comparative evaluation, concluding this effort in early 1979. A second ad hoc team then used the checklist to review implementation plans during the approximate period April through August 1979, completing the preliminary review. The OMB "Agency Computer Security Program Checklist" is appended as Appendix F, along with an OMB-generated list of policies and other computer security references. Initial OMB-identified plan deficiences were communicated to departments and agencies, primarily on an informal basis.

OMB intends to continuously and actively monitor Executive Branch department and agency implementation of TM1 to OMB circular A-71 through the following vehicles: (1) through review of agency budget submissions, where ADP security

is to be a specific item of concern during the course of the budget process*; (2) through ongoing OMB monitorship of Privacy Act implementation; (3) and through the reports clearance process (e.g. the Federal Reports Act) wherein unclassified, sensitive information within the scope of TM1 can be identified.

Information Security Oversight Office

The Information Security Oversight Office (ISOO) was established by Executive Order 12065 to actively oversee the information security program established by that Executive Order. As such, it replaced the Interagency Classification Review Committee (ICRC) established by the preceding Executive Order 11652 and is to be viewed as an attempt to incorporate a more viable mechanism to ensure that Executive Branch agencies were effectively implementing the program (a problem addressed, for example, in a GAO report of March 9, 1979, entitled "Improved Executive Branch Oversight Needed for the Government's National Security Information Classification Program"). Under EO 12065, the ISOO is required to monitor the program of any Executive Branch agency that handles classified national security information (in contrast to the ICRC's monitoring of only those 37 agencies then having original classification authority), so that the ISOO must now monitor approximately 100 agencies and major components. Also in response to other ICRC problems (placement and lack of independent stature), the ISOO was located within the General Services Administration for administrative purposes, but takes it policy direction from the National Security Council. During the transition between the two Executive Orders, the former ICRC Executive Director became the Acting ISOO Director and the ICRC staff of eight formed the nucleus of the new ISOO. By August 1979, a permanent Director had been appointed and the ISOO staff reached eleven. Since then, five program analysts joined the staff. This staff augmentation will allow the ISOO to conduct in-depth studies of various aspects of the security field. Included in these studies will be an examination of the use of ADP systems in the information security field. It is anticipated that the initial phases of this study will be completed in Fiscal Year 1981. In its first annual report to the President, the ISOO indicated that they conducted 123 inspections for which a formal report was written [32]. These covered 52 agencies plus 25 major components and 25 staff offices of those agencies, as well as three inspections of field activities outside the Washington metropolitan area. The ISOO staff also conducted 18 follow-up inspections. In carrying out its oversight role, the ISOO also reviews the implementing regulations of all monitoring agencies and requires such changes as may be necessary to achieve compliance with the provisions of Executive Order 12065 and its implementing ISOO Directive.

*Subcommittee members note that there is no current mechanism in agency budget submissions to identify expenditures other than research & development (R&D) efforts being conducted by agency computer security R&D elements as such. Accordingly, this mechanism is less effective in potential than it appears at face value since other ADP security-related R&D and ADP security operations and maintenance funding would not be identified. Furthermore, survey findings show this item to have the least frequency of positive responses in policy documents reviewed (c f., p. 8).

Inspector General/Internal Audit

Another set of potential though general program oversight mechanisms lies in the Congressional establishment of additional internal investigative functions in Executive Branch agencies and departments. Legislation enacted in the 94th and 95th Congresses provided for the creation of inspector general offices in most Federal departments and agencies (i.e., P.L. 94-505 for HEW; P.L. 94-452 for 21 other Federal departments and agencies and P.L. 95-1 for DOE). Such an entity for the Defense Department is still under active consideration.

Programs to Combat Fraud & Waste in the Executive Branch

The President's initiative to attack fraud and waste in the Federal Government also served to focus attention on computer security as well as the internal audit, inspection and investigative functions. In Defense, for example, a high level Steering Group was formed in 1978 to respond to the President's initiative and to improve the oversight of Defense activities. Noteworthy is the fact that the initial Defense report to the President [33] identified computer fraud as an important facet of the overall program as well as summarizing DoD Component ADP security programs and Defense's Computer Security Initiative Program.

Under the Steering Group, a computer fraud subcommittee was formed under the Under Secretary of the Air Force. Its report to the Steering Group in May 1979 [34] specifically recommended that computer security technology being developed within Defense to protect classified information should be applied to computer fraud, with Defense taking a lead in this application. To parallel the development of policy and procedures for limiting computer fraud, recommendations were made to provide a stable level of funding for DoD Computer Security Initiative Program [44,45] technology efforts under the Assistant Secretary of Defense (Communications, Command, Control & Intelligence), based upon the belief that the computer technology being developed to protect classified information would be applicable to combatting fraud (e.g., the methodologies for designing and verifying that internal computer system controls are effective). The Steering Group accepted the recommendations and the identified initial funding was allocated, however, out-year funding has not been confirmed.

Information on other department/agency programs pursuant to the President's initiative was not obtained.

It is noted that should some version of the proposed "Federal Computer Systems Protection Act" be enacted, that would in all probability serve to significantly reinforce pursuit of this initiative within the Executive Branch.

GAO Follow-up --

Recent Reports and Activities. In 1977, GAO surveyed selected agencies due to the high level of congressional interest in Federal information policies. This review included 10 civil agencies, but excluded the area of national security information in Defense agencies. Particular attention was given to agencies' efforts to organize and implement broad programs of data security in compliance with OMB Directives and related computer security guidelines published by the National Bureau of Standard (Appendix A).

A GAO report reflected the results of the survey, and it is entitled, "Automated Systems Security - Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data" [35], dated January 3, 1979. The GAO report indicated that all agencies reviewed had some elements of a computer security program in varying stages of existence, however, they generally lacked the management support needed to be truly comprehensive. With specific reference to OMB Circular A-71, TM 1, GAO concluded that since the document is both directive and quite comprehensive, it sets an appropriate framework for agencies' initiatives to correct computer security problems. It recommended to OMB concern for a critical need for OMB follow-up on the Circular's requirement that agencies prepare and submit plans for compliance.

Highlighted recommendations to the heads of Federal departments and agencies to improve computer security included the following:

-- Computer security programs should be comprehensive and include plans, policies and procedures clearly establishing organizational responsibilities in writing.

-- A computer security administration function should be established with independence from computer operations and should report directly to or through a principal official who reports directly to the head of the organization.

-- Programs should provide for feedback to management, both in routine monitoring/reporting and in independent internal audit.

-- Risk management should be provided for, on a total data systems perspective.

-- Security planning should anticipate needs for training, especially in risk management.

The report cited above excluded Defense Components, deferring the latter due to known, on-going internal audits. In a GAO letter report to the Secretary of Defense in March, 1979, [36] GAO noted the foregoing, stated that GAO had subsequently identified and analyzed 106 computer security-oriented audits related to over 270 facilities and/or systems and also reviewed Department of Defense and components' computer security programs and guidelines. GAO stated that this review demonstrated that the Department of Defense and its Components have experienced difficulties in each of the broad areas discussed in the Jan 1979 report, cited above.

Partial Policy/Program Integration

Many of the diverse activities and mechanisms cited above are (or can be) effectively integrated, as suggested by the OMB comments on the 1979 GAO report cited above [35]. OMB specifically advised that the GAO information and recommendations would be used in their own assessments of Federal agencies' plans to comply with Circular A-71 and other requirements. OMB further cited a high priority on improving agencies' security programs, noted it has organized a task force to review agencies' plans, and that this effort is coupled with noted broader concerns for improving controls over fraud and waste. Further noted by OMB was the indication that agencies' inspector general functions will also focus on correcting these matters in recognition of their importance as key responsibilities of agency and department heads.

1980 GAO Evaluation

During 1980, GAO has been performing a followup evaluation of implementation of the recommendations from its January 1979 report cited above. This is in response to a request from the Chairman, Subcommittee on Government Information and Individual Rights, House of Representatives Committee on Government Operations. The report will focus on:

1. OMB and central agency roles previously discussed (pp. 12-14, above); and,

2. Department/agency progress in implementing the security plans required by TM 1.

It is expected that the results of the review will be completed by November 30, 1980.

An interim letter report on this evaluation [46] noted the announced OMB reorganization of its Information Systems Policy Division and Regulatory Policy and Management Division into the Office of Regulatory and Information Policy. The report indicates the new office will have three divisions: Regulatory Policy, Reports Management and Information Policy. The new Office will include a "desk officer" responsible for monitoring the implementation of regulatory, reports management, and information management activities in each assigned department or agency. Relevant to computer security, the report further states:

> OMB advised us that many of the desk officers know little about automatic data processing in general or automated security in particular. OMB, realizing that these officers need training and help from people knowledgeable about automated security, plans to conduct such training during May and June 1980. Effective monitoring by trained OMB staff is necessary if the intent of the memorandum--security of automated information systems--is to be met.

V. POLICY IMPACTS -- AN AGENCY PERSPECTIVE

There are additional considerations from a policy perspective, beyond merely the presence or absence of policy as such, or the presence or absence of program oversight. Some of these will be briefly explored by viewing the context and flow of computer security policies as they impact a large Executive Branch organization, the Department of Defense.

The organization is by most criteria large -- in terms of number of personnel, budget size, and organizational complexity as historically evolved. Most significant here, however, is the magnitude of use of computer systems in support of departmental mission accomplishment, as a key arm of the national security establishment. As noted previously, just in terms of general purpose, commercially available ADP systems alone, DoD accounts for about 50% of the GSA inventory. In addition, DoD owns and/or operates literally uncounted numbers of special purpose computer systems (e.g., computers embedded in weapons and other systems). Moreover, the DoD has responsibility, derived from an Executive Order and executive agreements with other Executive Branch Agencies and Departments, to assume security program administration on behalf of sixteen such departments and agencies for contractors handling classified national security information.

A point of the example is to illustrate the manner in which computer security policies and associated requirements converge on an Executive Branch organization and a fashion in which they can be integrated (or not be integated) The overall situation is one which carries the potential for the generation of confusion, unwarranted duplication of effort, and policy conflict. The duplication concern is particularly critical inasmuch as computer security is a relatively new area requiring attention, to include resources. And existing resources appear to be quite limited, particularly in the face of the dramatic expansion of requirements represented by the scope of the recently promulgated OMB requirements.

Current Policies and Sources of Requirements

Classified Information. DoD programs for computer security are in implementation of and must be consistent with requirements imposed by higher authorities. Beginning with the classified arena, the most pertinent generic authority imposing security responsibilities upon the Secretary of Defense is Executive Order 12065 [10] as amplified by Information Security Oversight Office Directive Number 1 [37] (Figure 7).

Particularly relevent to implementation of the order in the ADP environment is the information classification scheme; namely, that national security information or material shall be classified in one of three categories, TOP SECRET, SECRET, or CONFIDENTIAL and no other categories shall be used except as expressly provided by statute.

While the Executive Order focused primarily on the classification and declassification of national security material and improving the balance between the two competing principles of informing the public and preserving confidentiality, it also contains other pertinent, broad and generic security

DEVELOPMENT AND IMPLEMENTATION OF ADP SECURITY POLICY

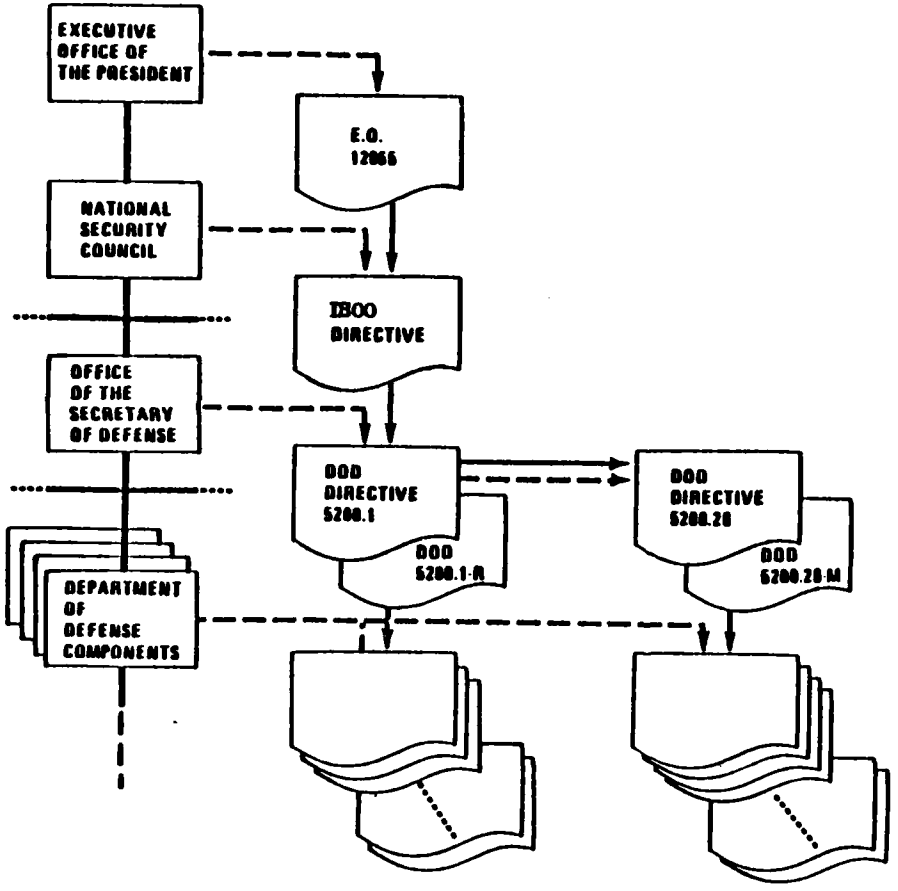


Figure 7

policy requirements, most of which present problematic judgments when applied to the ADP arena.

As these requirements are implemented by formal issuances down the indicated organizational chains of command, they are elaborated upon and generally specified as appropriate to more limited organizations and environments. There are also built-in feedback or oversight mechanisms for the evaluation of lower-level implementations. For example, in OSD, all DoD Component implementating documents must be reviewed and formally certified as being consistent with the basic DoD issuance.

The E.O. does not address computers per se. DoD's primary implementation, the Information Security Program Regulation, DoD 5200.1-R[4], does not either, except for paragraphs dealing with various media that may be associated with computer processing (e.g., punched cards, printouts, micro-forms). DoD Directive 5200.28 [1] in essence represents DoD's implementation of the E.O. insofar as the relatively unique problems posed by shared computer systems are concerned. The relationship between the two cannot be understated because much of the overall security guidance to be applied to the ADP environment is in 5200.1-R and is simple not duplicated in 5200.28. Therefore, in implementing policy, reference to both 5200.28 and 5200.1-R is required.

Defense's ADP security program policies impact not only the DoD Components but also those ADP systems processing classified information among the 11,000 contractors in the Defense Industrial Security Program (Figure 8). As mentioned, this Program is administered by DoD on behalf of sixteen other Executive Branch Departments and Agencies, in addition to the DoD Components, and currently identified industrial ADP systems (over 2,000) represent a significant number of the total ADP systems subject to DoD ADP security policies.

Special Access Programs. So far the flow of implementation of policy is fairly straight forward. But there is always an "other," and as shown, there are basically four sets of "Special Access Programs" that impact the Information Security Program (Figure 9):

NATO, where ADP security procedures are based on International Treaty Requirements;

Requirements concerning access to and dissemination of Restricted Data and Critical Nuclear Weapon Design Information;

Special Access Programs for Foreign Intelligence or other information under the cognizance of the Director of Central Intelligence or the National Communications Security Committee; and

DoD "Special Access Programs" as such.

DoD policy in this area is to utilize the standard classification categories to limit access to classified information on a "need-to-know" basis to personnel who have been determined to be trustworthy pursuant to the E.O. and ISOO Directive so that there will be no need to resort to formal special Access Programs (e.g., requiring extraordinary procedures and controls, such as

DEVELOPMENT AND IMPLEMENTATION OF ADP SECURITY POLICY

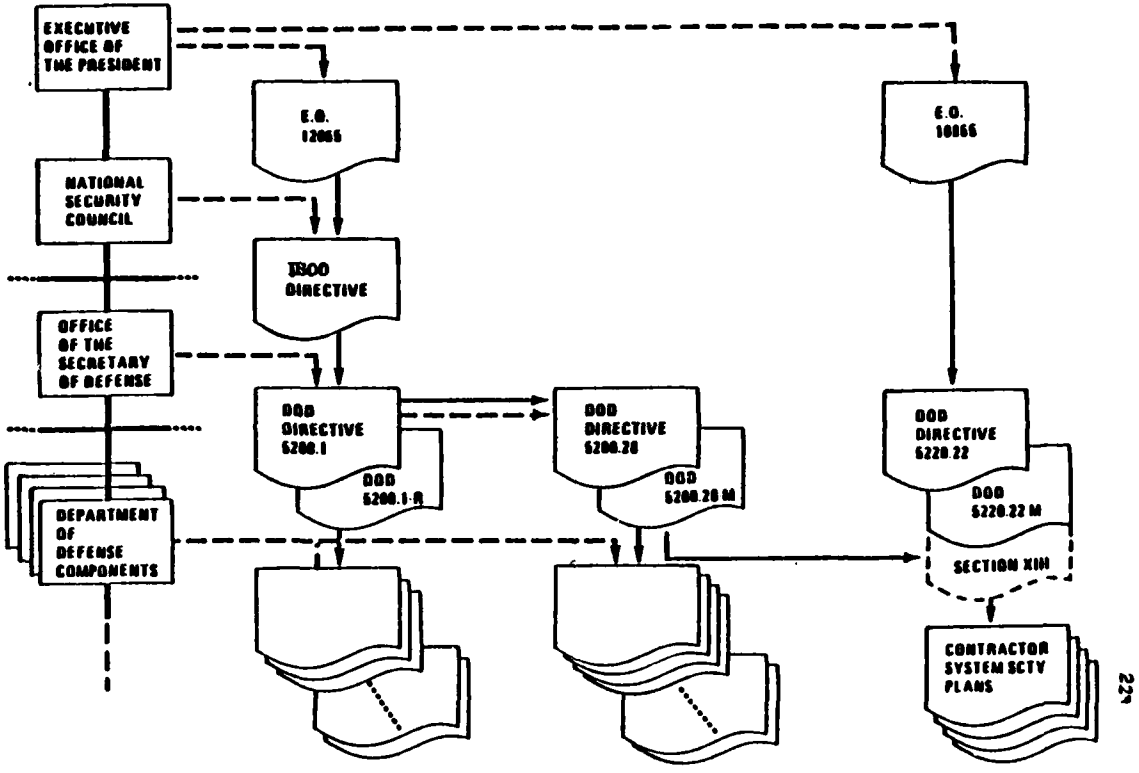


Figure 8

DEVELOPMENT AND IMPLEMENTATION OF ADP SECURITY POLICY

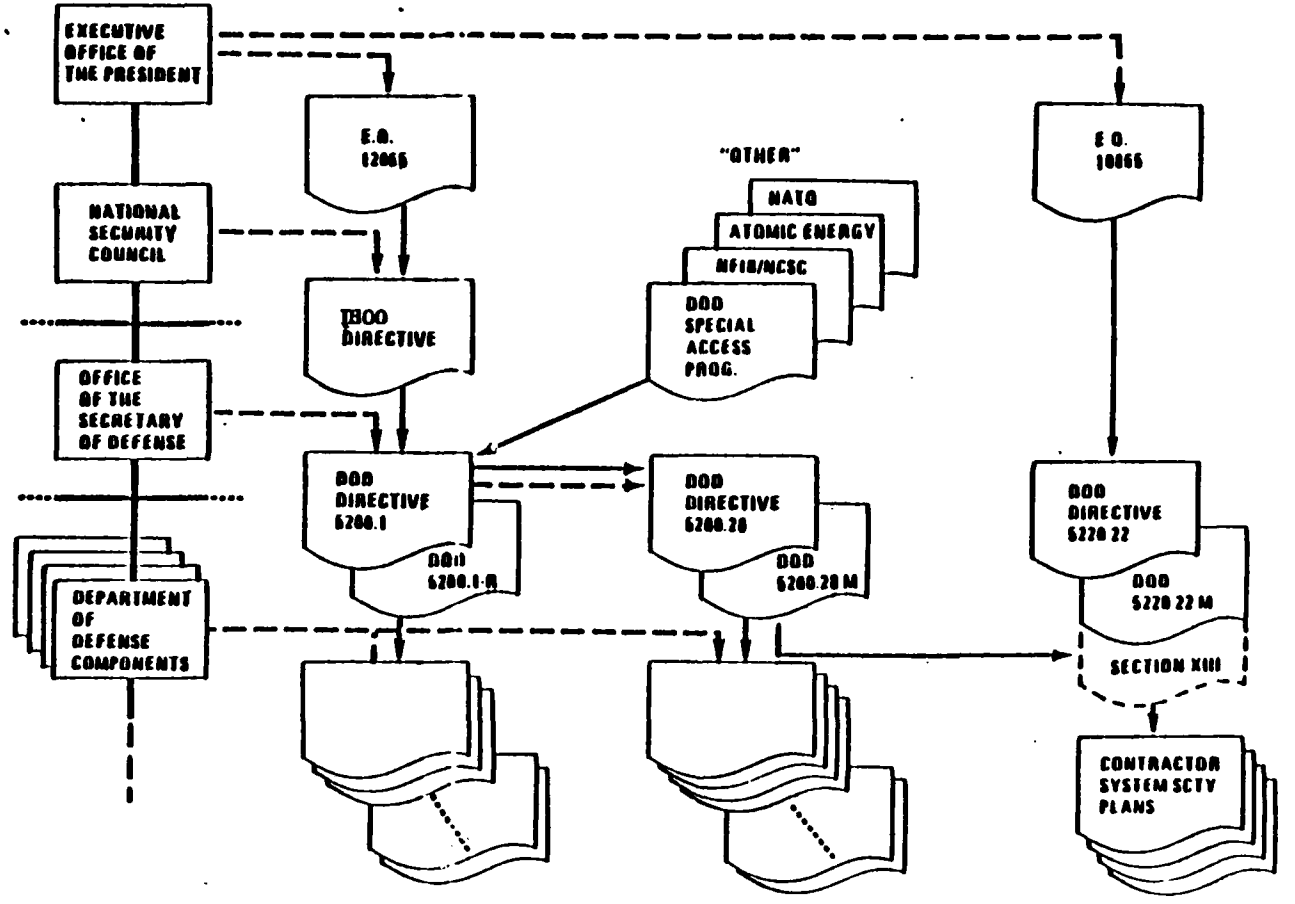


Figure 9

formal access determination, special briefings, reporting procedures, and recorded formal access lists.) Where such programs do exist, however, they are signficant potential sources of additional security requirements in various areas which must be considered in both system security planning and in policy development, integration and implementation. Noted as particularly significant is the necessity at the Federal department/agency level to effectively integrate diverse classified information protection policies from difference sources, and then further effectively integrate that result with emerging computer system protection requirements from newer sources, such as the following.

Privacy. Implementation of the Privacy Act of 1974 (Public Law No. 93-579, U.S.C. 552a) was implemented through a DoD Directive and concurrent establishment of a DoD Privacy Board [38], (Figure 10). With regard to computer security as such, current DoD policy consists of rather specific interim guidelines [39]. These will be superceded by a comprehensive DoD Regulation now under development to establish uniform Defense policy concerning interpretation and implementation of the Privacy Act. One of its chapters will contain specific policies for "Safeguarding Personal Information in ADP Systems."

TM 1 to OMB A-71 (Figure 11). DoD's approach to implementing these responsibilities specifically seeks to comprehensively integrate various computer security programs. The approach being pursued is one of essentially applying to the A-71 requirements the ADP security policy framework that has evolved in the classified arena over approximately the past decade. Essentially DoD envisions first categorization of data and applications on the basis of criteria analogous to those that exist for classified national security information. Secondly, ADP systems are primarily categorized in terms of the data/applications processed, and then specific security requirements are directly derived, primarily on a system basis. Incorporated is the multi-disciplinary, systematic approach to implementation that characterizes the classified arena. A third essential ingredient is utilization of the currently authorized system security modes (Figure 12).

The data and application sensitivity categories that have been proposed are amplified in Appendix H.

This conceptual scheme was included in the DoD plan submitted to OMB and concurrently in the memorandum promulgating the plan within Defense, appropriately entitled, "A Comprehensive Information Security Program" [40]. The plan further notes that, notwithstanding existing policies that satisfy some TM-1 requirements, new or modifed guidance is required. Pending development of such guidance, the TM-1 policies should be considered to have full force and effect, as amplified in the memorandum.

Policy & Program Oversight

Classified Information. Already mentioned was the fact that DoD Component implementations are reviewed against basic DoD policy, and each Component implementing issuance (Figure 13) must be reviewed and certified in writing as being consistent with the basic policy issuance, or corrective action must be taken.

DEVELOPMENT AND IMPLEMENTATION OF ADP SECURITY POLICY

(NONCLASSIFIED INFORMATION)

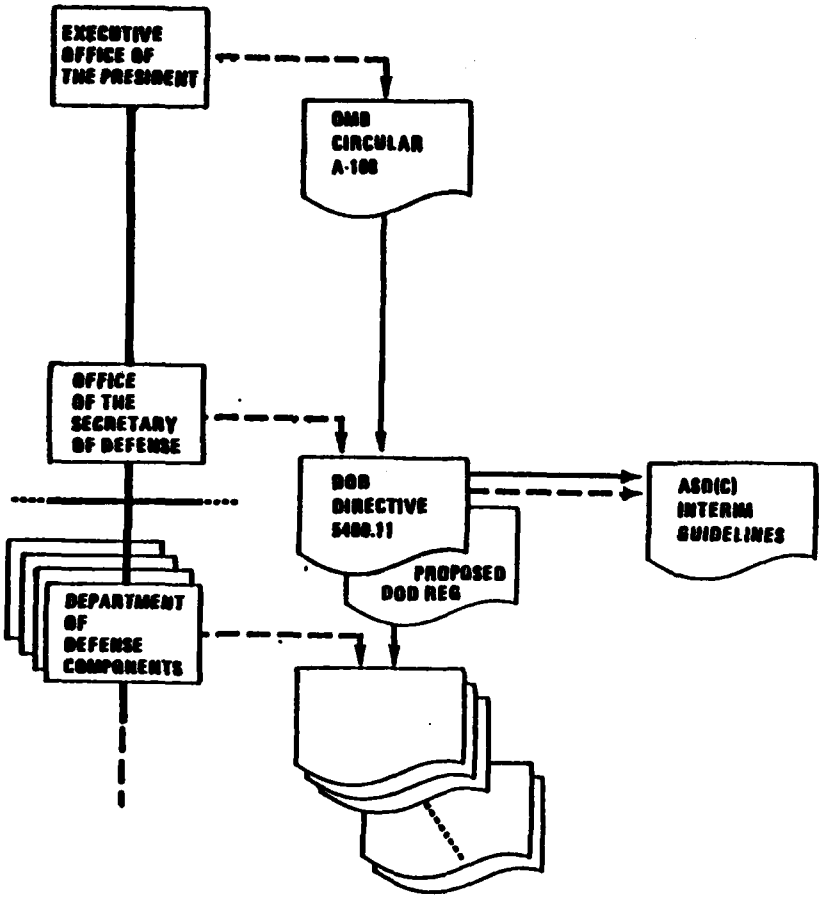


Figure 10

DEVELOPMENT AND IMPLEMENTATION OF ADP SECURITY POLICY

(NONCLASSIFIED INFORMATION)

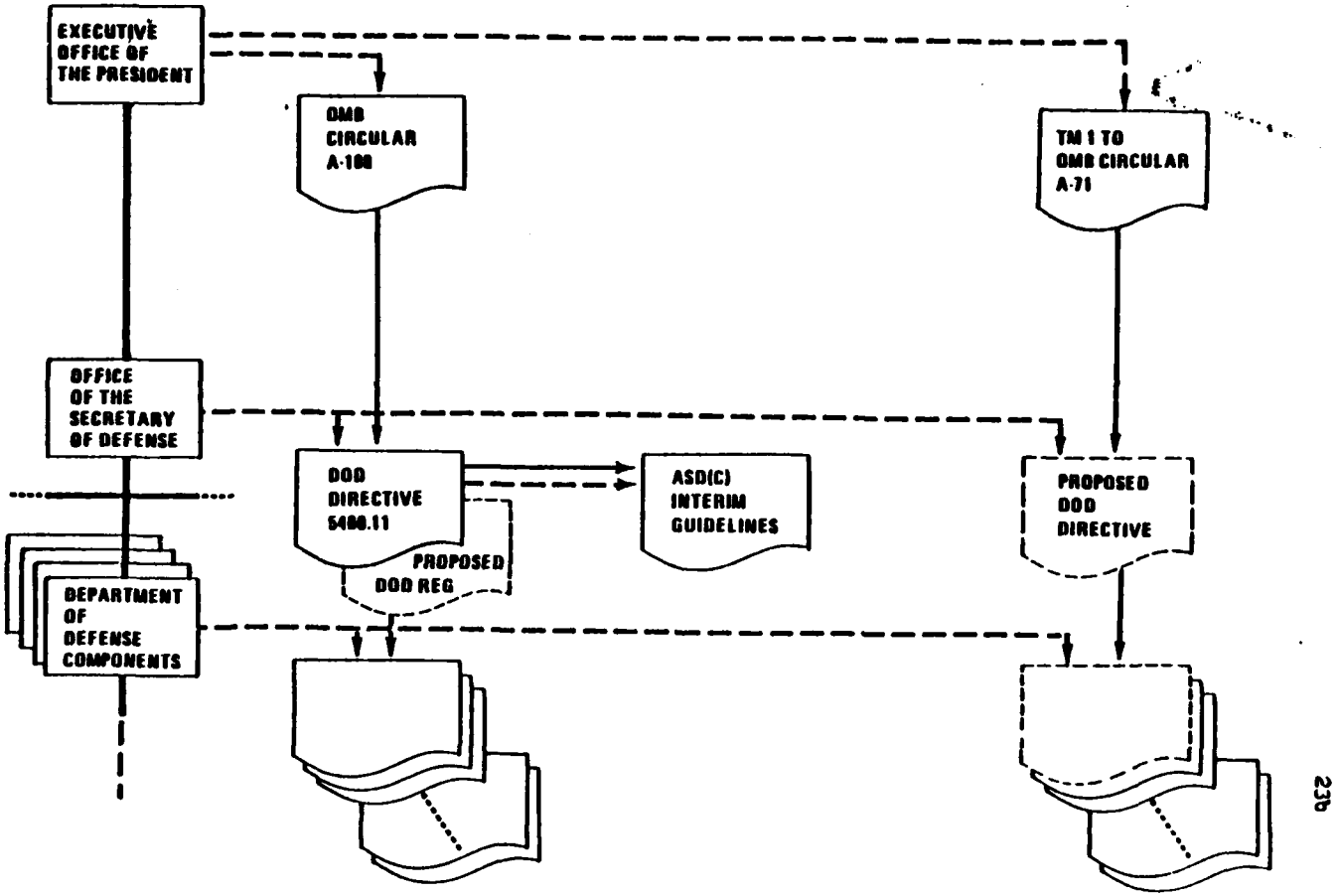


Figure 11

POLICY CONCEPT

- CATEGORIZE: DATA/APPLICATIONS; SYSTEMS
- INCORPORATE MULTI-DISCIPLINARY, SYSTEMS APPROACH
- EMPLOY CURRENT SYSTEM SECURITY MODES

TM 1 TO OMB CIRC. A-71
CATEGORIZE:

- DOD DATA & APPLICATIONS
- SYSTEMS
- POSITIONS

Figure 12

DOD COMPONENT IMPLEMENTATIONS

DOD DIRECTIVE 5200.28

DEPARTMENT OF THE ARMY	AR 380-380
DEPARTMENT OF THE NAVY	OPNAVINST 5239.1
DEPARTMENT OF THE AIR FORCE	AFR 300-8
JOINT CHIEFS OF STAFF	SM-150-73 (SM-635-77)
DEFENSE COMMUNICATIONS AGENCY	DCA Instruction 630-230-19
DEFENSE CONTRACT AUDIT AGENCY	DCAA Manual 5205.1
DEFENSE INTELLIGENCE AGENCY	DIAR 50-23
DEFENSE LOGISTICS AGENCY	DIAR 5200.5
DEFENSE MAPPING AGENCY	DMAINST 5200.28A
DEFENSE NUCLEAR AGENCY	DNA INST 5200.28A
NATIONAL SECURITY AGENCY	NSA/CSS Dir. No. 10-27
DEFENSE INDUSTRIAL SECURITY PROGRAM	DOD Manual 5220.22-M

(Jan 80)

Figure 13

Complementary on-site "information security oversight visits" are undertaken by the Office of the Secretary of Defense (OSD) to assess the field implementation of policy. Some of these on-site oversight visits have specifically addressed computer security matters, both among the DoD Component and among contractor facilities included within the Industrial Security Program. Additional oversight visits more intensely focusing on computer security as such are specifically programmed for the current and forthcoming Fiscal Years.

Additional oversight activities are conducted under the auspices of various special access programs included within the DoD Information Security Program. For example, the Defense Intelligence Agency conducts security inspections of other DoD Components' facilities for compliance with policy where certain categories of "sensitive compartmented information" are being handled, including contractor facilities, and the NATO Office of Security annually conducts inspections of 15 NATO member nations' security arrangements for the protection of NATO classified information.

Further oversight is provided through the medium of internal audit, for example, Defense Audit Service (DAS) evaluations and reports and Inspector General reports.

Privacy. Component implementations of DoD policy implementing the requirements of the Privacy Act are likewise subject to formal policy certification by OSD.

Additionally, on-site oversight visits to selected ADP installations were also undertaken by OSD in conjunction with this program.

Lastly, a multitude of internal audits were undertaken concerning privacy and other computer security considerations at selected activities within the Defense Agencies and Military Departments (e.g., DAS "Summary Report on the Audit of ADP Systems Security and Privacy at Selected Defense Data Processing Installations," [41] -- Appendix G lists activities included in the audit reports and specific audit reports issued).

TM 1 to OMB A-71. Although no specifics are now in place concerning oversight of implementation of this program (which is currently being developed within Defense), it is probable that at least the policy certification and internal audit functions will provide policy and program oversight in the department.

Summary Comments

The foregoing suggests one problem for a Federal department or agency implementing computer security requirements imposed by diverse higher echelon authorities -- integrating these requirements into a relatively homogeneous, consistent and coherent internal policy framework (Figure 14). In the Defense Department example, this was essentially accomplished within the classified arena by integrating minimum classified information protection requirements with those additional and often different requirements for classified "Special

DEVELOPMENT AND IMPLEMENTATION OF ADP SECURITY POLICY

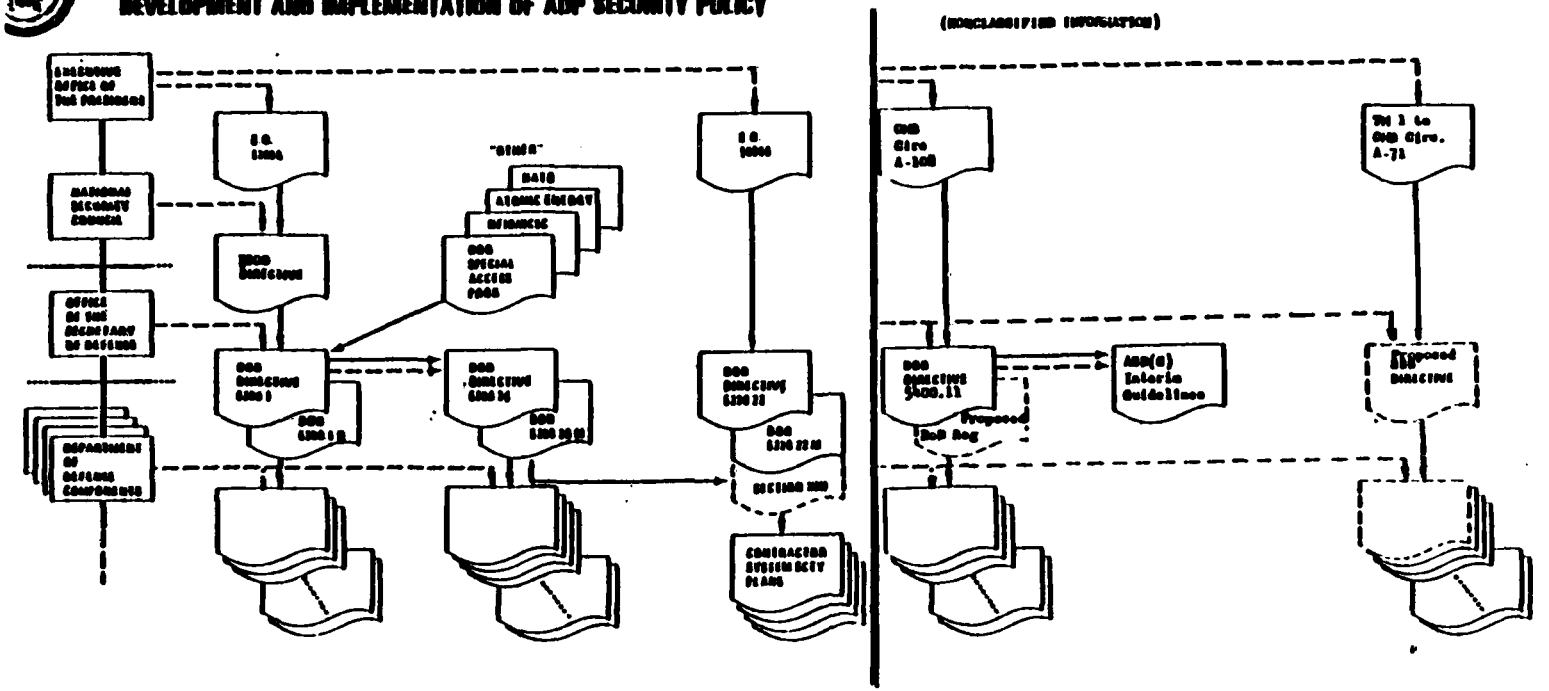


Figure 14

Access Program" information comprehensively. The approach appears to work well.*

By contrast, there has been little linkage between classified computer security policy and policy stemming from departmental implementation of requirements from the Privacy Act of 1974 and OMB Circular A-108.

The subsequent promulgation of TM 1 to OMB A-71 serves to integrate computer security policies and progams, to include field implementation.

The general point, beyond the Defense example, is that explicit attention must be given to the impact at the department/agency level of higher level actions, particularly the derivative and cascading effects of any policy confusion, conflict, inconsistencies and ambiguities from the top down to the bottom line -- the ultimate implementation of policies in field data processing installations.

* Even this is not without potential problems however. For example, one Special Access Program for intelligence includes in its scope all intelligence, not just "compartmented" or otherwise "Special Access-type" intelligence. For the non-compartmented intelligence handled within DoD, the DCI's policy may in the future directly conflict with those of the Secretary of Defense (imposed for classified information per se by E.O. 12065 [10]) if the respective policies, where they intersect, come to differ.

VI. SUMMARY, CONCLUSIONS & INFERENCES

Federal Department/Agency Level

Of the fifteen Executive Branch departments and agencies surveyed, representing over 88% of the Federal computer systems reflected in the GSA inventory, all had promulgated computer security policies in effect. These varied, however, in scope, applicability and approach.

Specifically revealed and reviewed were 32 documents meeting the criteria set forth herein as computer security policies, and these provided essentially 27 policy document sets (1,316 pages) associated with the fifteen agencies. The policies involved differences in overall approach (e.g., combination or separation of policies stemming from different authoritative sources), scope (e.g., classified information, non-classified information, personal information) and applicability (e.g., include internal components and/or contractors).

Primary authoritative bases on the basis of frequency cited among the 27 policy sets were:

o	EO 12065	63%
o	Privacy Act	41%
o	TM 1 to A-71	30%
o	Intelligence Special Access Programs	30%
o	EO 10865	15%
o	National COMSEC Dir	15%
o	OMB Circular A-108	11%
o	Atomic Energy Act	7%

"National" Level

Derived from the foregoing, the survey clearly reflected:

o Omnibus Policy. In place, comprehensive computer security policy promulgated by the Office of Management and Budget, Executive Office of the President [7].

o This policy explicity includes:

-- all Federal data and applications processed by computer systems

-- personal, proprietary and other sensitive data not subject to national security regulations as well as national security data

-- such data/applications processed by Federal computer systems as well as by other systems on behalf of Federal departments and agencies

o Pursuant to OMB central agency tasking under this program policy:

-- OPM has issued personnel security requirements and guidelines now in the Federal Personnel Manual [22,23];

-- GSA has amended the Federal Property Management Regulations (FPMR amendment F-42) to add a new section for the protection of ADP and telecommunications systems and a subpart to provide guidelines on environmental and physical security of ADP facilities [25];

-- GSA has amended the Federal Procurement Regulations (FPR Amendment 210) to require that agencies' computer security requirements be included and certified in agency procurement requests and that acquisition specifications include certified Government computer security requirements in connection with solicitations, contracts, and contract administration [26]; and,

-- National Bureau of Standards, Department of Commerce, has issued numerous information and guidance publications on computer security [6] as well as maintaining an ongoing program for standards development.

o Other Policies. There are also documented herein a number of other, earlier Executive Branch-level computer security policies of narrower scope and applicability, including:

-- Department/agency-generated policies in implementation of generic classified information safeguarding requirements imposed by Executive Order 12065

-- Special Access Program classified information, such as:

- NATO information
- Intelligence information
- Restricted Data and associated information

-- Policies associated with implementation of the Privacy Act of 1974 in the ADP arena and OMB Circular A-108.

The interrelationships of these policies are suggested by the diagrams at Figures 15 and 16. Figure 15 shows these as separately promulgated from the national level; Figure 16 relates them in a Venn context wherein the OMB policy includes all Federal data/applications processed by computers.

Oversight Results

However, audits and associated reviews (e.g., [27], [28], [29], [30], [31], [35], and [41]) have found significant problems with the field implementation of computer security programs.

Most recent is the January 1979 GAO report which concluded that "programs fell short of being comprehensive and top management support was lacking"

NATIONAL LEVEL AUTHORITATIVE BASES FOR COMPUTER SECURITY POLICIES

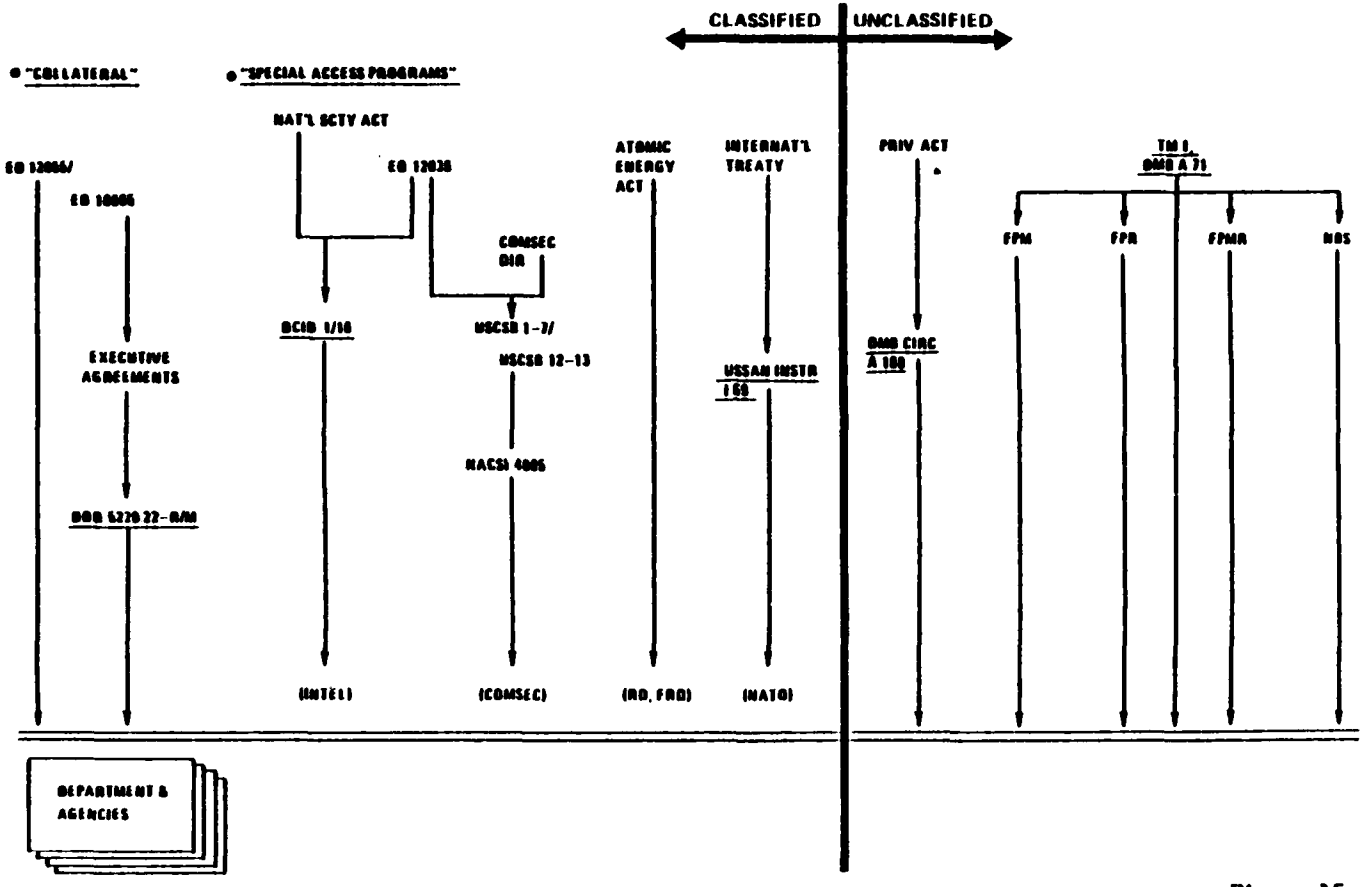
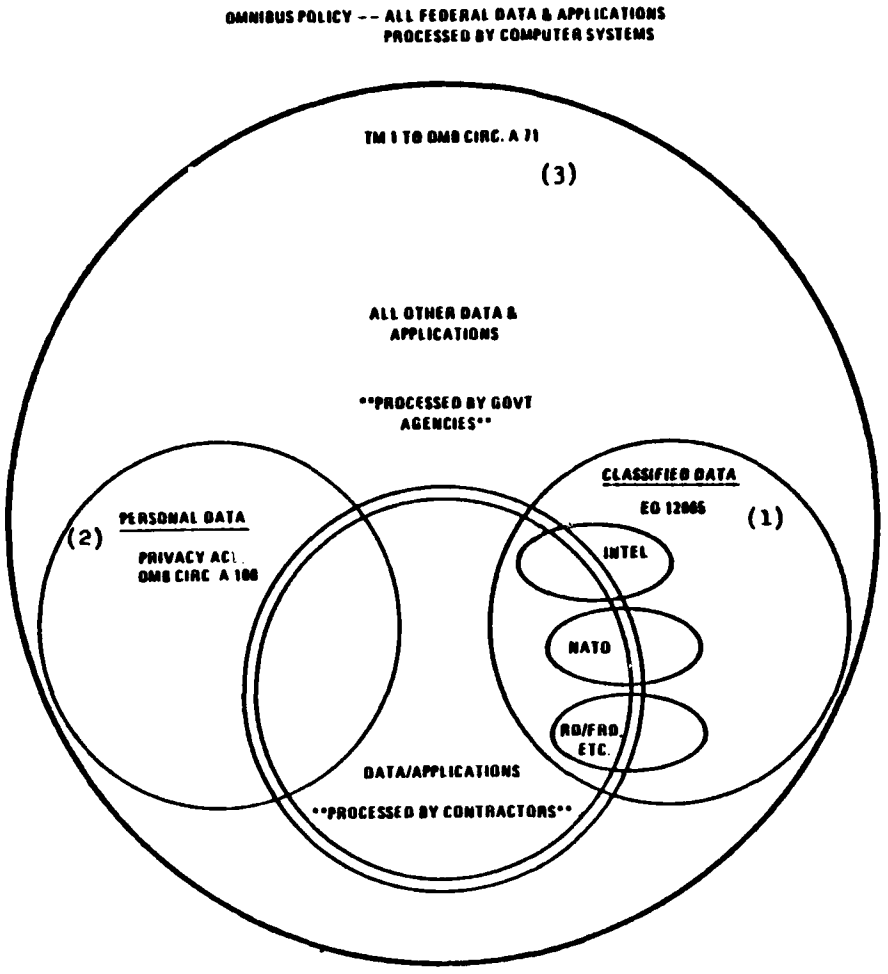


Figure 15

(Underlining denotes documents meeting the criteria herein for computer security policies)

FEDERAL AUTOMATED INFORMATION AND COMPUTER SECURITY POLICY SETS



(3) Protect data & applications from disclosure, alteration, destruction, misuse or other loss or harm (e.g. fraud, waste, crime and unecessary or improper actions)

(2) Protect data from unwarranted intrusions upon individual privacy

(1) Protect data from unauthorized disclosure

Figure 16

[35] (emphasis added). The report noted that the review was completed prior to the issuance of TM 1 to OMB Circular A-71, but noted that the document "...requires action by top agency managers which could contribute greatly to correcting many of the computer data security problems addressed in the GAO report." Further, "...it (TM 1 to A-71) sets an appropriate framework for agencies' initiatives to correct their data security problems."

The "Digest" to this GAO report is attached for reference as Appendix I.

Conclusions

The Subcommittee considers the current situation to suffer significantly from fragmentation across-the-board and from the lack of cost effective, feasible implementing guidance. The former particularly is manifest in the example of national policy flow and impacts at the department/agency level (pp.22-26). This suggests a clear need for further efforts to effectively integrate overall computer security policies in a context that specifically considers the flow of data/applications to be protected, 1. between and among Federal agencies, and 2. between Federal agencies and private sector contractors.

The foregoing in turn, indicates that a deeper level of analysis is required to focus on those aspects of computer security field implementation that are susceptible to benefit from national level attention and effort.

Accordingly, the Subcommittee strongly and unanimously recommends attention be given to the following specific problem areas related to current computer security policies and field implementation thereof:

1. The nature, magnitude and practical effects of the lack of top management support in Federal Departments and Agencies ([35] and Appendix I), to specifically include the need for the education and awareness of top management on the many facets of computer security and the interrelationships of computer security with other programs and functional activities;

2. Closely interrelated with the foregoing, lack of resources, to include both research and development resources and operational resources, with specific attention to the problem of trained manpower and funding stability;

3. Intensive focus on the problematic nature of the hardware/software computer security subdiscipline (e.g., [42], [43], [44], and [45]), to specifically include the development of secure systems technology, security technical evaluation methodologies and mechanism(s), and recommended management and operational mechanism(s) thereof;

4. Manifest requirements for means of more effective integration and coordination of identified national policy promlgating activities (see Figures 15 & 16 as well as conflict examples on pp. 13 & 25).

5. Generation of feasible and cost-effective implementing guidance for various computer security subdisciplines associated with the implementation of overall computer security policies (in addition to 3., above, highlighted examples include communications security guidance specifically keyed to computer systems and networks and similar tailored emanations security guidance).

REFERENCES

1. "Security Requirements for Automatic Data Processing (ADP) Systems," Department of Defense Directive 5200.28, December 18, 1972, as amended (Change 2, April 29, 1978).

2. "ADP Security Manual" Techniques and Procedures for Implementing, Deactivating, Testing and Evaluating Secure Resource-Sharing ADP Systems," Department of Defense Manual DoD 5200.28-M, January 1973, as amended (Change 1, June 25, 1979).

4. "Information Security Program Regulation," Department of Defense Regulation DoD 5200.1-R, December 1978.

5. "COMSEC Guidance for ADP Systems" (U), National COMSEC/EMSEC Information Memorandum No. 7002, September 1975 (CONFIDENTIAL).

6. Computer Security Publications, NBS Publications List 91, National Bureau of Standards, U.S. Department of Commerce, revised June 1980.

7. "Security of Federal Automated Information Systems," Transmittal Memorandum No. 1 to OMB Circular No. A-71, Office of Management and Budget, Executive Office of the President, Washington, D.C. 20503, July 27, 1978.

8. Automatic Data Processing Equipment Inventory in the United States Government, Automated Data and Telecommunications Service, General Services Administration, April 1979.

9. "Responsibilities for the Maintenance of Records About Individuals by Federal Agencies." OMB Circular No. A-108, Office of Management and Budget, Executive Office of the President, Washington, D.C. 20503, July 1, 1975, as amended (Transmittal Memorandum No. 5, August 3, 1978).

10. "National Security Information," Executive Order 12065, The Federal Register, July 3, 1978.

11. "ADP Systems Security," Part 6, Chapter 6-00, Department of Health, Education & Welfare ADP Systems Manual, as amended (1978).

12. "ADP Security and Privacy," Chapter 6, Department of Agriculture "Departmental Information Processing Standards," February 25, 1977, as amended (Amendment 6, March 31, 1980).

13. "Security Requirements for ADP Systems," Section XIII, "Industrial Security Manual for Safeguarding Classified Information," Department of Defense Manual DoD 5220.22-M, April 17, 1980.

15. "Implementation of NATO Security Procedure (U)," United States Security Authority for NATO Affairs Instruction 1-69, December 17, 1973, as amended (revised, Dec. 1, 1979) (Enclosure to DoD Instruction C-5210.21, same subject) (CONFIDENTIAL).

16. "Safeguarding Classified Information Within Industry," Executive Order 10865, February 20, 1960, as amended (E.O. 10909).

17. "Security Requirements for Classified Automatic Data Processing Systems," Department of Energy Order 5636.2, January 10, 1980, and "Computer Security Guidelines for Classified Automatic Data Processing Systems," DOE Manual 5636.2, March 1980.

18. "Security of Automatic Data Processing Systems," Part XII, Appendix 2101 to U.S. Nuclear Regulatory Commission NRC Manual, March 29, 1979.

20. "Security of Compartmented Computer Operations" (U), Chapter 8, "Sensitive Compartmented Information (SCI) Contractor Administrative Security Volume II (U)," Defense Intelligence Agency, Washington, D.C. 20301, October 22, 1979.

21. Office of Management and Budget, Executive Office of the President, News Release # OMB - 29, OMB Information Office, July 28, 1978.

22. "Personnel Security Program for Positions Associated with Federal Computer Systems," FPM (Federal Personnel Manual) Letter 732-7, Office of Personnel Management, Washington, D.C. 20415, November 14, 1978 (Subsequently incorporated in the Federal Personnel Manual as Section 9, Subchapter 1, Chapter 732).

23. "Authorities and Guidelines for Investigations of Persons Having Access to Federal Computer Systems and Information in Those Systems," Federal Personnel Manual Bulletin 732-2, Office of Personnel Management, Washington, D.C. 20451, January 11, 1980.

24. "Security Requirements for Government Employment," Executive Order 10450 April 27, 1953, as amended.

25. "Security of Federal ADP and Telecommunications Systems," Federal Property Management Regulations Amendment F-42, 41 CFR CH. 101, The Federal Register, August 11, 1980.

26. "Special Types and Methods of Procurement; Automatic Data Processing Contracting," Federal Procurement Regulations Amendment 210, 41 CFR Part 1-4, The Federal Register, October 6, 1980.

27. "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government," U.S. General Accounting Office, Washington, D.C. 20013, Report FGMSD-76-5 (April 23, 1976).

28. "Computer-Related Crimes in Federal Programs," U.S. General Accounting Office, Washington, D.C., Report FGMSD-76-27 (April 27, 1976).

29. "Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities," U.S. General Accounting Office, Washington, D.C., Report FGMSD-76-40 (May 10, 1976).

30. "Problems Associated with Computer Technology in Federal Programs and Private Industry--Computer Abuses," Committee on Government Operations, U.S. Senate, June 1976.

31. "Staff Study of Computer Security in Federal Programs," Committee on Government Operations, U.S. Senate, February 1977.

32. "Information Security Oversight Office Annual Report to the President -- Fiscal Year 1979," Information Security Oversight Office, General Services Administration, Washington, D.C. 20405, April 21, 1980.

33. "Department of Defense Programs to Prevent and Detect Fraud and Waste in Government Operations," Department of Defense Report to the President, submitted to the Office of Management and Budget, January 31, 1979.

34. "Recommendations for Employing Computer Security Technology to Combat Computer Fraud," Computer Subcommittee Report to the DoD Steering Group on Oversight of Defense Activities, May 1979.

35. "Automated Systems Security -- Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data," U.S. General Accounting Office, Washington, D.C., Report LCD-78-123 (January 23, 1979).

36. U.S. General Accounting Office Letter Report to the Secretary of Defense concerning automated systems security programs in DoD, Report LCD-79-109, March 21, 1979.

37. "Information Security Oversight Office Directive No. 1 Concerning National Security Information," Information Security Oversight Office, General Services Administration, The Federal Register, October 5, 1978.

38. "Personal Privacy and Rights of Individuals Regarding Their Personal Records," Department of Defense Directive 5400.11, August 4, 1975.

39. "Interim Policy on Safeguarding Personal Information in ADP Systems," Assistant Secretary of Defense (Comptroller) memorandum to the Military Departments and Defense Agencies, April 26, 1978.

40. "A Comprehensive Information Security Program," Assistant Secretary of Defense (Comptroller) multi-addressee Memorandum, January 30, 1980.

41. "Summary Report on the Audit of ADP Systems Security and Privacy at Selected Defense Data Processing Installations," Report No. 952, Defense Audit Service, September 29, 1978.

42. Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security, published by the Rand Corporation for the Office of the Director of Defense Research and Engineering (Rand Report #R-609), February 11, 1970.

43. Stryker, D.J., "Subversion of a 'Secure' Operating System," Naval Research Laboratory, Washington, D.C. 20375, NRL Memorandum Report 282 (June 1974).

44. Proceedings of the Seminar on the DoD Computer Security Initiative Program, National Bureau of Standards, Gaithersburg, Maryland, July 17-18, 1979.

45. Proceedings of the Second Seminar on the DoD Computer Security Initiative Program, National Bureau of Standards, Gaithersburg Maryland, January 15-17, 1980.

46. GAO Letter Report B-198551, Subject: "Central Agencies' Compliance With OMB Circular A-71," Transmittal Memorandum No. 1 (LCD-80-56-I), April 30, 1980.

COMPUTER SECURITY PUBLICATIONS

NBS Publications List 91

Revised June 1980

U.S. Department of Commerce
National Bureau of Standards
Institute for Computer Sciences and Technology

APPENDIX A

APPENDIX A

COMPUTER SECURITY PUBLICATIONS

These computer security publications have been issued by the Institute for Computer Sciences and Technology of the National Bureau of Standards. They cover techniques, practices, and policies for protecting computers and data from unauthorized and undesirable modification, disclosure or destruction. A glossary of terms related to computer security is included on page 15.

How to Order Publications

These publications are available through the Government Printing Office (GPO) and the National Technical Information Service (NTIS). The source and price for each publication are indicated. Orders for publications should include title of publication, NBS publication number (Spec. Pub. 000, Tech. Note 000, etc.) and NTIS or GPO number. You may order at the price listed; however, prices are subject to change without notice.

Submit payment in the form of postal money order, express money order or check made out to the Superintendent of Documents for GPO-stocked documents or to the National Technical Information Service for NTIS-stocked documents.

Mailing addresses are:

Superintendent of Documents
U. S. Government Printing Office
Washington, D. C. 20402

National Technical Information Service
5285 Port Royal Road
Springfield, Virginia 22161

Telephone numbers for information are:

GPO Order Desk	(202) 783-3238
NTIS Orders	(703) 557-4700
NTIS Information	(703) 557-4600

About ICST

The Institute for Computer Sciences and Technology

- develops federal computer standards and guidelines for efficient utilization and procurement of computers by federal agencies and departments;
- provides technical assistance and advice to federal agencies in the selection and use of computers;
- performs computer science research to support standards development and advisory activities.

For information about Federal Information Processing Standards and other computer-related publications, you may write to:

Institute for Computer Sciences and Technology
A200 Administration
National Bureau of Standards
Washington, D. C. 20234

AUDIT AND EVALUATION

Audit and Evaluation of Computer Security
Edited by Zella Ruthberg and Robert McKenzie
NBS Spec. Pub. 500-19 October 1977

Order from GPO as SN 003-003-01848-1 $4.00

Reports on the recommendations of audit and computer experts to improve computer security audit procedures. Subjects covered include audit standards, administrative controls, program and data integrity, and audit tools and techniques.

Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls
Edited by Zella G. Ruthberg
NBS Spec. Pub. 500-57 April 1980

Order from GPO as SN 003-003-02178-4 $6.00

Proceedings of the second NBS/GAO workshop to develop improved computer security audit procedures. Contains the findings of three managerial and five technical sessions on computer system vulnerabilities and controls.

Guidelines for Automatic Data Processing Risk Analysis
FIPS PUB 65 August 1979

Order from NTIS as NBS FIPS-PUB-65 $4.50

Presents a technique for conducting a risk analysis of an ADP facility and related assets. Provides guidance on collecting, quantifying, and analyzing data related to the frequency of occurrence and the damage caused by adverse events. A specific example is given.

CRYPTOGRAPHY

A Key Notorization System for Computer Networks
By Miles E. Smid
NBS Spec. Pub. 500-54 October 1979

Order from GPO as SN 003-003-02130-0 $1.75

Describes a system for key notorization, which can be used with an encryption device, to improve data security in computer networks. The key notorization system can be used to communicate securely between two users, communicate via enrypted mail, protect personal files, and provide a digital signature capability

Computer Security and the Data Encryption Standard
Edited by Dennis Branstad
NBS Spec. Pub. 500-27 February 1978

Order from GPO as SN 003-003-01891-1 $3.00

Includes papers and summaries of presentations made at a 1977 conference on computer security. Subject areas are physical security, risk assessment, software security, computer network security, applications and implementation of the Data Encryption Standard.

Data Encryption Standard
FIPS PUB 46 January 1977

Order from NTIS as NBS FIPS-PUB-46 $3.50

Specifies a mathematical algorithm to be implemented in electronic hardware devices and used for the cryptographic protection of computer data.

Report of the Workshop on Cryptography in Support of Computer Security
By Dennis Branstad, Jason Gait and Stuart Katzke
NBSIR 77-1291 September 1977

Order from NTIS as PB 27144 $5.25

Reports on a workshop held at NBS to obtain expert opinions on the mathematical and statistical characteristics of the Data Encryption Standard. Summarizes the formal presentations and outlines the major issues that were raised.

Report on the Workshop on Estimation of Significant Advances in Computer Technology
Edited by Paul Heisenberg
NBSIR 76-1189 December 1976

Order from NTIS as PB 279373 $4.50

Reports on a 1976 workshop held to solicit information on computer technology advances with potential impact on the security of the Data Encryption Standard. Presents the evaluations of computer industry, academic and government experts on computer system design, architecture and manufacturing.

Technical Specifications of a Proposed Federal Information Processing Standard on the Modes of Operation for the Data Encryption Standard
By Michael J. O'Brien
NBSIR 80-2019 April 1980

Order from NTIS as PB 80-183189 $6.00

Describes four implementation techniques for using the Data Encryption Standard for the cryptographic protection of sensitive, but unclassified, computer data.

Validating the Correctness of Hardware Implementations of the NBS Data Encryption Standard
By Jason Gait
NBS Spec. Pub. 500-20 November 1977

Order from GPO as SN 003-003-01861-9 $1.60

Describes the design and operation of the NBS testbed that is used for the validation of hardware implementations of the Data Encryption Standard (DES). This report provides the full specification of the DES algorithm, a complete listing of the DES test set and a detailed description of the interface to the testbed.

DATA BASE SECURITY

A Data Base Management Approach to Privacy Act Compliance
By Elizabeth Fong
NBS Spec. Pub. 500-10 June 1977

Order from GPO as SN 003-003-01787-6 $1.40

Discusses how data base management systems can be used to implement Privacy Act requirements for the handling of personal data.

Data Base Directions: The Next Steps
Edited by John Berg
NBS Spec. Pub. 451 September 1976

Order from GPO as SN 003-003-01662-4 $3.00

Proceedings of a workshop held in 1975 to develop information about data base technology for managers of data base systems. Covers five subject areas: auditing, evolving technology, government regulations, standards and user experience.

GENERAL COMPUTER SECURITY

Accessing Individual Records from Personal Data Files Using Nonunique Identifiers
By Gwendolyn B. Moore, John L. Kuhns, Jeffrey L. Treffzs and Christine A. Montgomery
NBS Spec. Pub. 500-2 February 1977

Order from GPO as SN 003-003-01726-4 $2.65

Analyzes methodologies for retrieving personal information using nonunique identifiers such as name, address, etc. This study presents statistical data for judging the accuracy and efficiency of various methods.

Approaches to Privacy and Security in Computer Systems
Edited by Clark Renninger
NBS Spec. Pub. 404 September 1974

Order from GPO as SN 003-003-01319-6 $1.45

Reports on a conference held at NBS to propose ways to meet government needs in safeguarding individual privacy and confidentiality of data. The views of legislators, citizens, computer industry associations and companies, professional societies, and public interest groups are presented.

Government Looks at Privacy and Security in Computer Systems
Edited by Clark Renninger and Dennis Branstad
NBS Tech. Note 809 February 1974

Order from NTIS as COM 74-50174 $4.50

Reports on a conference held at NBS to identify the legal, technological and administrative needs and problems of government agencies in safeguarding individual privacy and protecting confidential data from loss or misuse.

Controlled Accessibility Bibliography
By Susan K. Reed and Martha Gray
NBS Tech. Note 780 June 1973

Order from NTIS as COM 73-50533 $4.00

A bibliography of 96 references to literature about computer security.

Controlled Accessibility Workshop Report
By Susan K. Reed and Dennis Branstad
NBS Tech. Note 827 May 1974

Order from NTIS as COM 74-50457 $5.00

Reports on technical meeting dealing with computer access controls, security audits, ADP management controls, personal identification and security assessments.

Glossary for Computer Systems Security
FIPS PUB 39 February 1976

Order from NTIS as NBS FIPS-PUB-39 $3.50

Includes terms related to privacy and computer system security.

Guidelines for Automatic Data Processing Physical Security and Risk Management
FIPS PUB 31 June 1974

Order from NTIS as NBS FIPS-PUB-31 $5.00

A handbook for structuring physical security and risk management programs for ADP facilities. Covers security analysis, natural disasters, failure of supporting utilities, system reliability, procedural measures and controls, protection of off-site facilities, contingency plans, security awareness and security audit.

Guidelines for Documentation of Computer Programs and Automated Data Systems
FIPS PUB 38 February 1976

Order from NTIS as NBS FIPS-PUB-38 $4.50

Presents guidelines on the documentation needed at each stage of the software life cycle to provide for cost effective operation, revision and maintenance.

Operating System Structures to Support Security and Reliable Software
By Theodore Linden
NBS Tech. Note 919 August 1976

Order from GPO as SN 003-003-01658-6 $1.25

Examines techniques to improve the design of computer systems. This study focuses on two system structuring concepts using modular software structures to satisfy security requirements and make systems more reliable.

Performance Assurance and Data Integrity Practices
By Robert L. Patrick
Edited by Robert P. Blanc
NBS Spec. Pub. 500-24 January 1978

Order from GPO as SN 003-003-01879-1 $2.20

Details, practices and methods that have been successful in preventing or reducing computer system failures caused by programming and data errors. The methods described cover large data processing applications, scientific computing applications, programming techniques and systems design.

Security Analysis and Enhancements of Computer Operating Systems
Edited by Theodore Linden
NBSIR 76-1041 April 1976

Order from NTIS as PB 257087 $4.50

Examines types of security problems that arise in operating systems and suggests ways to improve security. Three commercial systems are analyzed, and security flaws are classified.

NETWORK SECURITY

Design Alternatives for Computer Network Security (vol. 1)
The Network Security Center: A System Level Approach to Computer Network Security (vol. 2)
By Gerald D. Cole and Frank Heinrich
NBS Spec. Pub. 500-21 January 1978

Order from GPO as SN 003-003-01881-3 $6.00

This two-volume study covers network security requirements and design and implementation requirements of a special computer dedicated to network security. It focuses on use of the Data Encryption Standard to protect network data and recommends procedures for generating, distributing and protecting encryption keys.

PERSONAL IDENTIFICATION AND ACCESS AUTHORIZATION

Evaluation of Techniques for Automated Personal Identification
FIPS PUB 48 April 1977

Order from NTIS as NBS FIPS-PUB-48 $4.00

Discusses techniques for identifying individuals seeking access to computer systems. This report presents data for measuring the effectiveness of personal identification devices and for evaluating techniques and devices.

The Use of Passwords for Controlled Access to Computer Resources
By Helen Wood
NBS Spec. Pub. 500-9 May 1977

Order from GPO as SN 003-003-01770-1 $2.00

Describes the need for and uses of passwords. Password schemes are categorized according to selection technique, lifetime, physical characteristics and information content.

PRIVACY

A Computer Model to Determine Low Cost Techniques to Comply With the Privacy Act of 1974
By Robert C. Goldstein and Henry H. Seward
NBSIR 76-985 February 1976

Order from NTIS as PB 250755 $4.50

Presents a computer model to simulate costs of implementing the Privacy Act and to identify differences in cost that result from alternative approaches to implementing mandated safeguards.

A Data Base Management Approach to Privacy Act Compliance
By Elizabeth Fong
NBS Spec. Pub. 500-10 June 1977

Order from GPO as SN 003-003-01787-6 $1.40

Discusses how data base management systems can be used to implement Privacy Act requirements for the handling of personal data.

A Methodology for Evaluating Alternative Technical and Information Management Approaches to Privacy Requirements
By Robert C. Goldstein, Henry M. Seward and Richard L. Nolan
NBS Tech. Note 906 June 1976

Order from GPO as SN 003-003-01630-6 $1.35

Identifies the actions required of recordkeepers to comply with the Privacy Act and estimates the cost of these actions. Includes a computer model to aid in the selection of cost-effective safeguards.

Approaches to Privacy and Security in Computer Systems
Edited by Clark Renninger
NBS Spec. Pub. 404 September 1974

Order from GPO as SN 003-003-01319-6 $1.45

Reports on a conference held at NBS to propose ways to meet government needs in safeguarding individual privacy and confidentiality of data. The views of legislators, citizens, computer industry associations and companies, professional societies, and public interest groups are presented.

Computer Security Guidelines for Implementing the Privacy Act of 1974
FIPS PUB 41 May 1975

Order from NTIS as NBS FIPS-PUB-41 $3.50

Describes physical security, information management practices, and computer system security controls that can be used by Federal ADP organizations to implement computer security safeguards.

Computers, Health Records, and Citizen Rights
By Alan F. Westin
NBS Monograph 157 December 1976

Order from GPO as SN 003-003-01681-1 $4.55

Reports on the impact of computers on citizen rights in the health recordkeeping area. This study looks at the uses made of personal medical data and the trends in computerization of data. It recommends policy actions to guide the management of health data systems that respect citizen rights.

Computers, Personnel Administration, and Citizen Rights
By Alan F. Westin
NBS Spec. Pub. 500-50 July 1979

Order from GPO as SN 003-003-02087-7 $8.00

Report on the impact of computers on citizen rights in the field of personnel recordkeeping. This study traces the changing patterns of employment and personnel administration and examines the trends in computer use in personnel administration. It recommends policy actions to guide the management of personnel systems that respect citizen rights.

A Policy Analysis of Citizen Rights Issues in Health Data Systems
By Alan F. Westin and Florence Isbell
NBS Spec. Pub. 469 January 1977

Order from GPO as SN 003-003-01730-2 $1.05

A condensation of "Computers, Health Records, and Citizen Rights" (Monograph 157).

Exploring Privacy and Data Security Costs--A Summary of a Workshop
Edited by John Berg
NBS Tech. Note 876 August 1975

Order from NTIS as COM 75-11113 $4.50

Reports on workshop discussions about the cost of complying with the Privacy Act. Subjects covered include identifying costs, both direct and indirect, identifying benefits from implementing Privacy Act requirements, and allocating costs among those who receive benefits.

Index of Automated System Design Requirements as Derived from the OMB Privacy Act Implementation Guidelines
NBSIR 75-909 October 1975

Order from NTIS as PB 246863 $3.50

Lists requirements to be considered by administrative and technical personnel in complying with Privacy Act provisions relating to automated systems design and development.

SECURITY CONTROLS AND SAFEGUARDS

An Analysis of Computer Security Safeguards for Detecting and Preventing Intentional Computer Misuse
By Brian Ruder and J. D. Madden
Edited by Robert P. Blanc
NBS Spec. Pub. 500-25 January 1978

Order from GPO as SN 003-003-01871-6 $2.40

Analyzes 88 computer safeguard techniques that could be applied to recorded actual computer misuse cases. Presents a model for use in classifying and evaluating safeguards as mechanisms for detecting and preventing misuse.

Computer Security Guidelines for Implementing the Privacy Act of 1974
FIPS PUB 41 May 1975

Order from NTIS as NBS FIPS-PUB-41 $3.50

Describes physical security, information management practices, and computer system security controls that can be used by Federal ADP organizations to implement computer security safeguards.

Considerations in the Selection of Security Measures for Automatic Data Processing Systems
By Michel J. Orceyre and Robert H. Cortney, Jr.
Edited by Gloria B. Bolotsky
NBS Spec. Pub. 500-33 June 1978

Order from GPO as SN 003-003-01946-1 $1.40

Details, methods and techniques for protecting data processed by computer and transmitted via telecommunications lines. This report identifies the controls that can be instituted to protect ADP systems when risks and potential losses have been identified.

Government Looks at Privacy and Security in Computer Systems
Edited by Clark Renninger and Dennis Branstad
NBS Tech. Note 809 February 1974

Order from NTIS as COM 74-50174 $4.50

Reports on a conference held at NBS to identify the legal, technological and administrative needs and problems of government agencies in safeguarding individual privacy and protecting confidential data from loss or misuse.

Guidelines for Automatic Data Processing Physical Security and Risk Management
FIPS PUB 31 June 1974

Order from NTIS as NBS FIPS-PUB-31 $5.00

A handbook for structuring physical security and risk management programs for ADP facilities. Covers security analysis, natural disasters, failure of supporting utilities, system reliability, procedural measures and controls, protection of off-site facilities, contingency plans, security awareness and security audit.

Operating System Structures to Support Security and Reliable Software
By Theodore Linden
NBS Tech. Note 919 August 1976

Order from GPO as SN 003-003-01658-6 $1.25

Examines techniques to improve the design of computer systems. This study focuses on two system structuring concepts using modular software structures to satisfy security requirements and make systems more reliable.

Performance Assurance and Data Integrity Practices
By Robert L. Patrick
Edited by Robert P. Blanc
NBS Spec. Pub. 500-24 January 1978

Order from GPO as SN 003-003-01879-1 $2.20

Details, practices and methods that have been successful in preventing or reducing computer system failures caused by programming and data errors. The methods described cover large data processing applications, scientific computing applications, programming techniques and systems design.

Security Analysis and Enhancements of Computer Operating Systems
Edited by Theodore Linden
NBSIR 76-1041 April 1976

Order from NTIS as PB 257087 $4.50

Examines types of security problems that arise in operating systems and suggests ways to improve security. Three commercial systems are analyzed, and security flaws are classified.

GLOSSARY

(excerpted from FIPS PUB 39, Glossary for Computer Systems Security)

Audit	Independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy or procedures.
Confidentiality	A concept that applies to data that must be held in confidence; describes the status and degree of protection that must be provided for such data about individuals as well as organizations.
Controlled Accessibility	Process of limiting access to the resources of an ADP system only to authorized users, programs, processes or other ADP systems (in computer networks).
Cryptography	The principles, means and methods for rendering plain text unintelligible and for converting encrypted messages into intelligible form.
Data Security	The protection of data from accidental or malicious modification, destruction or disclosure.
Physical Security	The use of locks, guards, badges and other administrative measures to control access to the computer and related equipment; the measures required for the protection of the structures housing the computer, related equipment and their contents from damage by accident, fire and environmental hazards.
Privacy	The right of individuals and organizations to control the collection, storage and dissemination of their information or information about themselves.
Security	Protection for hardware, software and data.

SURVEY

EXECUTIVE BRANCH COMPUTER SECURITY POLICY DOCUMENTS

1. DEPARTMENT/AGENCY PROMULGATING THE DOCUMENT: _____

2. DOCUMENT IDENTIFICATION (Please complete questionnaire for draft documents if there is not yet an approved, published version of the same scope & applicability):

   a. Title (of document or that part/section dealing with computer security):

   _____

   b. Regulation or other Number, where applicable: _____

   c. Date (if revised, enter date of latest revision or change):

   _____

   d. Check here only if document is an unapproved, unpublished draft: _____

3. AUTHORITATIVE BASIS(ES) FOR POLICY (Please "X" all of the following that are explicitly cited as authority for the document; enter "0" for others that are cross-referenced for separate application):

   a. Pertaining to classified National Security Information:

      (1) Executive Order 12065, "National Security Information," June 28, 1978: _____

      (2) USSAN (United States Security Authority for NATO Affairs) Memorandum No. 1, "Implementation of NATO Security Procedure (U)," 17 Dec 1973, as amended (pertaining to NATO classified information): _____

      (3) Atomic Energy Act of 1954, as amended (Public Law 93-438, pertaining to "Restricted Data" & Formerly Restricted Data"): _____

      (4) Special access programs for "intelligence" (i.e. "Foreign intelligence" and "counterintelligence" per EO 12036, (8), below) under the cognizance of the Director of Central Intelligence (e.g. DCID No. 1/16): _____

      (5) Other Department/Agency Special Access Programs (e.g. Dept. of Defense --"Single Integrated Operational Plan-Extremely Sensitive Information/SIOP-ESI"): _____

      (6) Executive Order 10865, "Safeguarding Classified Information Within Industry," February 20, 1960, as amended: _____

      (7) Presidential Directive/NSC-24 ("PD-24"), 16 Nov 77: _____

      (8) Executive Order 12036, "United States Intelligence Activities," January 26, 1978: _____

(9) "National Communications Security Directive (U)," 20 Jun 1979: _____

b. Pertaining to Unclassified Information:

(1) Privacy Act of 1974 (Public Law 93-579, 5 U.S. C. 552a): _____
and/or;
OMB Circular A-108, "Responsibilities for the Maintenance of Records About Individuals by Federal Agencies," July 1, 1975, as amended and supplemented: _____

(2) Transmittal Memorandum No. 1 to OMB Circular No. A-71, Security of Automated Information Systems," July 27, 1978: _____

(3) Records withheld from public disclosure under the Freedom of Information Act (5 U.S.C. 552): _____

c. Other General, Authoritative Bases:

(1) Prohibited Disclosure of confidential government information (18 U.S.C. 1905): _____

(2) Federal Reports Act - Unlawful disclosure of information; controlled release to other agencies (44 U.S.C. 3508): _____

(3) Unlawful personal use of public money, property or records (18 U.S.C. 641): _____

(4) Robbery of personal property of the U.S. (18 U.S.C. 2112): _____

(5) Injury or destruction of U.S. property (18 U.S.C. 1361): _____

(6) Willful, unlawful concealment, removal or mutilation of any record or other item filed with the U.S. (18 U.S.C. 2071): _____

(7) FPMR (Federal Property Management Regulation) 101-36.7, Management and Control of Computer Rooms and Related Support Areas," June 15, 1978: _____

(8) FPMR 101-35.17, "Privacy and Data Security for ADP and Telecommunications Systems," June 16, 1978: _____

(9) FPMR 101-34, "Emergency Preparedness Planning," June 16, 1978: _____

d. Other Authorities Cited -- Please identify fully as in 2., above, and attach the information to this questionnaire.

4. APPLICABILITY OF POLICY (Please "X" all that apply):

a. Applies to the department/agency identified in 1., above, and its components and facilities: _____

b. Applies to all (or most) department/agency contractors (i.e. any industrial, educational, commercial or other entity which has executed a contract with the department/agency): _____

5. PROTECTION SCOPE (Please "X" all that are included within the policy document):

a. Information/data

(1) Classified National Security Information: _____
and/or
Unclassified "National Security Related Information:" _____

(2) Personal information relating to individuals ("Privacy"): _____

(3) Other agency/department "sensitive information" and records: _____

b. (1) ADP systems (i.e. "Automatic Data Processing equipment," including computers and auxiliary or accessorial equipment such as I/O devices and communications equipment): _____

(2) Areas housing ADP systems or their components (e.g. physical areas containing main frame or remote terminals): _____

(3) Computer Programs (i.e. software) _____

(4) Other ADP resources and supplies: _____

c. Does the policy generally contain security requirements pertaining to the entire life cycle of ("X" if answer is "yes"):

(1) The ADP or computer systems concerned: _____

(2) Individual data/application systems: _____

6. COMPUTER SECURITY SUBDISCIPLINES SPECIFICALLY INCLUDED (Please "X" all requirement sets that are included in the policy document, to include requirements that may be enumerated in a separate document -- e.g. the computer security document requires personnel security or communications security actions set forth in a referenced, separate document):

a. Personnel Security: _____

b. Physical Security: _____

c. Communications Security: _____

d. Emanations Security: _____

e. Administrative/Procedural Security: _____

f. Hardware/Software Security: _____

7. PROGRAM COMPONENT ELEMENTS (Please "X" all that are included in essence within the document):

a. Assignment of Responsibility:

(1) For computer security within the Agency or Department (i.e. specification of a headquarters staff element as responsible for policy promulgation and program oversight): _____

(2) For specific ADP systems or ADP installations (e.g. Appointment of ADP System Security Officers): _____

b. Management Control Process to assure that administrative, physical, technical and other safeguards are included in agency computer systems: _____

c. Formally designated approving authority for the security aspects of covered ADP systems: _____

d. Overall security specifications/requirements: _____

e. Review, test and/or evaluation required as basis for system approval for operation: _____

f. Audit or other follow-up system or program security evaluations: _____

g. Risk Analysis or Risk Assessment methodologies _____

h. Security Requirements/Specifications Applicable to Procurement (i.e. equipment, systems or related services): _____

i. Requirements for Contingency Planning: _____

j. Personnel Screening Requirements _____

k. Specification of an authority to grant waivers: _____

l. Requirement to specify an ADP security budget: _____

8. APPROXIMATE NUMBER OF COMPUTER SYSTEMS COVERED BY POLICY (if known, for example, through agency submissions to GSA inventory): _____

9. NUMBER OF PAGES (single-spaced pages or equivalent): _____

10. QUESTIONNAIRE COMPLETED BY (Requested for purposes of follow-up only):

_____

Name Telephone Number

GUIDANCE FOR QUESTIONNAIRE COMPLETION

General.

Policy documents reviewed for purposes of this survey are to be only those documents (or parts of documents of larger scope) that treat computer security in a more or less complete sense. This includes both documents specifically on computer security and essentially complete in themselves (e.g. DoD Directive 5200.28 and DCID No. 1/16) as well as sections or parts of larger documents where the sections are essentially comprehensive computer security documents in themselves (e.g. Part 6 on computer security, which is a section of HEW's ADP Systems Manual, or Agriculture's "ADP Security and Privacy" chapter of their Departmental Information Processing Standards Manual).

By contrast, we are not interested for the moment in policy documents that contain provisions representing clearly incomplete, piecemeal elements associated with computer security. Examples here are Defense's Information Security Program Regulation, which includes security marking provisions for some ADP media, or Defense's directive on "Life Cycle Management of Automated Information Systems," which cites computer security requirements as a policy consideration--neither of these, however, set forth computer security policies in any comprehensive and enumerative sense.

It is recognized that subjective judgment is necessarily a part of completing the questionnaire. The primary consideration for survey purposes with regard to various policy attributes is presence or absence, not relative degree of completeness. For example, on question 7.a.(1), a policy document may assign program responsibility poorly (e.g. fragmented assignment to multiple organizational entities, with no one entity having overall responsibility), but it does assign computer security responsibilities. Also, inferences should be made if the words in the questionnaire do not clearly match verbiage in the document. For example, relating to question 5.c.(1), DoD Directive 5200.28 does not anywhere use the term "life cycle," but it does require that continued approval for processing classified information in an ADP system be based upon recurring security evaluation of the system. In this case, the question should be answered with an "X" since the provisions imply "cradle to grave" system security monitorship.

Please call if you have questions on borderline areas such as the foregoing, as this will help to assure consistency in the survey results.

Specific.

2. Essentially self-explanatory. However, where there is one document amplified or supplemented by another document of the same scope and applicability, please complete one copy of the questionnaire for both documents (e.g. DoD Directive 5200.28 and its companion manual DoD 5200.28-M, and DOE Order 5636.2 and its associated DOE Manual 5636.2).

3.a. Don't spend time hunting outside of the document itself for these. For DoD documents implementing DoD Directive 5200.28, however, the "X" should be entered for E.O. 12065, because the implementations are tertiary.

3.b.&c. "X" only those that are cited.

4.b. has been modified to indicate "all (or most) department/ agency contractors" in recognition of a provision in the Industrial Security Manual (covering DoD Component and 16 other Executive Branch department and agency classified information with contractors) that excludes only government-owned, contractor-operated systems located on government premises.

8. Unless easily found, leave blank, and I will enter this from the GSA Inventory where appropriate.

COMPUTER SECURITY POLICY DOCUMENTS REVIEWED

--Department/Agency Level Documents--

Department of Defense

DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems"
DoD Manual 5200.28-M, "ADP Security Manual--Techniques & Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems"
Assistant Secretary of Defense Comptroller Memorandum, "Interim Policy on Safeguarding Personal Information in ADP Systems"
Section XIII, "Security Requirements for ADP Systems," DoD Manual 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information"
DoD Manual C-5030.58-M, "Defense Special Security Communications System--Security Criteria and Telecommunications Guidance (U)"
Army Regulation 380-380, "Automated Systems Security"
OPNAVINST 5239.1, "Department of the Navy Security Program for Automatic Data Processing Systems"
Air Force Regulation 300-8, "Automated Data Processing System (ADPS) Security Policy, Procedures, and Responsibilities"
Air Force Regulation 300-13, "Safeguarding Personal Data in Automatic Data Processing Systems"
DIA Regulation 50-23, "Security Requirements for Automatic Data Processing (ADP) Systems"
DIA Manual 50-4, "Security of Compartmented Computer Operations (U)"
DIA Manual 50-5, "Sensitive Compartmented Information (SCI) Contractor Administrative Security -- Volume II (U)"
NSA/CSS Directive 10-27, "Security Requirements for Automatic Data Processing (ADP) Systems"
NSA/CSS Manual 90-4, "ADP Security Design and Operating Standards (U)"

Department of Energy

DOE Order 5636.2, "Security Requirements for Classified Automatic Data Processing Systems"
DOE Manual 5636.2, "Computer Security Guidelines for Classified Automatic Data Processing Systems"
DOE Order 1360.2, "Computer Security Program for Unclassified Computer Systems"

NASA

NASA Management Instruction 2410.7, "Assuring Security and Integrity of NASA Data Processing"

Department of Transportation

DOT Order 1640.7, "Department of Transportation Automatic Data Processing Security Policy"
DOT Order 1640.8, "Department of Transportation Automatic Data Processing Security" (DOT ADP Security Handbook)

Department of Treasury

DOT Order 102-3, "Personnel, Physical and Automatic Data Processing (ADP) Systems Security -- Organization and Delegation of Authority"
Treasury Directive 10-08, Part VII, "ADP Resource Protection"
Treasury Directive 10-08, Part VII, "ADP Privacy Act Guidelines"
Treasury Directive 10-08, Part VII, (DRAFT) "ADP Resource Protection Guidelines"

Department of HEW

Part 6, "ADP Systems Security," Chapter 6-00, HEW ADP Systems Manual

Department of Agriculture

Chapter 6, "ADP Security and Privacy," Departmental Information Processing Standards (DIPS) Manual
"ADP Security Handbook," USDA DIPS Manual Supplement

Department of Justice

DOJ Order 2640.2, "Automatic Data Processing (ADP) Security"

Nuclear Regulatory Commission

Part XII, "Security of Automatic Data Processing Systems," Appendix to NRC Manual Chapter 2101, "NRC Security Program"
Part XVII, "Automated Information Systems Security Program for Sensitive Data," Appendix to NRC Manual Chapter 2101

--National Level Documents--

Office of Management & Budget, Executive Office of the President

Transmittal Memorandum No. 1 to OMB Circular A-71, "Security of Federal Automated Information Systems", to include, by direction:

- ° Federal Personnel Manual Letter 732-7, "Personnel Security Program for Positions Associated with Federal Computer Systems," (Subsequently incorporated in the FPM as Section 9, Subchapter 1, Chapter 732)
- ° Federal Personnel Manual Bulletin 732-2, "Authorities and Guidelines for Investigations of Persons Having Access to Federal Computer Systems and Information in Those Systems"
- ° Amendment to Federal Property Management Regulations Part 101-35 to add 101.35.3, "Security of Federal ADP and Telecommunication Systems"
- ° Amendment to Federal Property Management Regulations, Subpart 101-36.7, retitled: "Environmental and Physical Security"
- ° Amendment to Federal Procurement Regulations to Section 1-4.1104, "Request for Procurement Action," to include computer security requirements
- ° Amendment to Federal Procurement Regulations to add Section 1-4.1107-21, "Computer Security Requirements"

OMB Circular A-108, "Responsibilities for the Maintenance of Records About Individuals by Federal Agencies"

U.S. Security Authority for NATO Affairs

Section X, "Protection of NATO Classified Information Handled and Stored in Automatic Data Processing Systems (U)," Enclosure 1 to USSAN Instruction 1-69, "Implementation of NATO Security Procedure (U)"

And Others

SUMMARY -- Executive Branch Departments & Agencies

- Total Agencies: 15
- Total documents: 32
- Total questionnaires: 27

SURVEY

EXECUTIVE BRANCH COMPUTER SECURITY POLICY DOCUMENTS

1. DEPARTMENT/AGENCY PROMULGATING THE DOCUMENT

2. DOCUMENT IDENTIFICATION

3. AUTHORITATIVE BASIS(ES) FOR POLICY

a. Pertaining to classified National Security Information:

(1) Executive Order 12065, "National Security Information," June 28, 1978: 17 (63%)

(2) USSAN (United States Security Authority for NATO Affairs) Memorandum No. 1, "Implementation of NATO Security Procedure (U)," 17 Dec 1973, as amended (pertaining to NATO classified information): 0

(3) Atomic Energy Act of 1954, as amended (Public Law 93-438, pertaining to "Restricted Data" & Formerly Restricted Data"): 2 (7%)

(4) Special access programs for "intelligence" (i.e. "Foreign intelligence" and "counterintelligence" per EO 12036, (8), below) under the cognizance of the Director of Central Intelligence (e.g. DCID No. 1/16): 8 (30%)

(5) Other Department/Agency Special Access Programs (e.g. Dept. of Defense --"Single Integrated Operational Plan-Extremely Sensitive Information/SIOP-ESI"): 0

(6) Executive Order 10865, "Safeguarding Classified Information Within Industry," February 20, 1960, as amended: 4 (15%)

(7) Presidential Directive/NSC-24 ("PD-24"), 16 Nov 77: 0

(8) Executive Order 12036, "United States Intelligence Activities," January 26, 1978: 2 (7%)

(9) "National Communications Security Directive (U)," 20 Jun 1979: 4 (15%)

b. Pertaining to Unclassified Information:

(1) Privacy Act of 1974 (Public Law 93-579, 5 U.S. C. 552a): 11 (41%)
and/or;
OMB Circular A-108, "Responsibilities for the Maintenance of Records About Individuals by Federal Agencies," July 1, 1975, as amended and supplemented: 3 (11%)

(2) Transmittal Memorandum No. 1 to OMB Circular No. A-71, Security of Automated Information Systems," July 27, 1978: 8 (30%)

(3) Records withheld from public disclosure under the Freedom of Information Act (5 U.S.C. 552): 2 (7%)

c. Other General, Authoritative Bases:

(1) Prohibited Disclosure of confidential government information (18 U.S.C. 1905): 1

(2) Federal Reports Act - Unlawful disclosure of information; controlled release to other agencies (44 U.S.C. 3508): 1

(3) Unlawful personal use of public money, property or records (18 U.S.C. 641): 1

(4) Robbery of personal property of the U.S. (18 U.S.C. 2112): 1

(5) Injury or destruction of U.S. property (18 U.S.C. 1361): 1

(6) Willful, unlawful concealment, removal or mutilation of any record or other item filed with the U.S. (18 U.S.C. 2071): 1

(7) FPMR (Federal Property Management Regulation) 101-36.7, Management and Control of Computer Rooms and Related Support Areas," June 15, 1978: 1

(8) FPMR 101-35.17, "Privacy and Data Security for ADP and Telecommunications Systems," June 16, 1978: 1

(9) FPMR 101-34, "Emergency Preparedness Planning," June 16, 1978: 0

d. Other Authorities Cited -- Please identify fully as in 2., above, and attach the information to this questionnaire.

4. APPLICABILITY OF POLICY (Please "X" all that apply):

a. Applies to the department/agency identified in 1., above, and its components and facilities: 25 (93%)

b. Applies to all (or most) department/agency contractors (i.e. any industrial, educational, commercial or other entity which has executed a contract with the department/agency): 23 (85%)

5. PROTECTION SCOPE (Please "X" all that are included within the policy document):

a. Information/data

(1) Classified National Security Information: and/or Unclassified "National Security Related Information:" — 21 (78%) / 8 (30%)

(2) Personal information relating to individuals ("Privacy"): — 16 (59%)

(3) Other agency/department "sensitive information" and records: — 14 (52%)

b. (1) ADP systems (i.e. "Automatic Data Processing equipment," including computers and auxiliary or accessorial equipment such as I/O devices and communications equipment): — 27 (100%)

(2) Areas housing ADP systems or their components (e.g. physical areas containing main frame or remote terminals): — 22 (82%)

(3) Computer Programs (i.e. software) — 24 (89%)

(4) Other ADP resources and supplies: — 17 (63%)

c. Does the policy generally contain security requirements pertaining to the entire life cycle of ("X" if answer is "yes"):

(1) The ADP or computer systems concerned: — 23 (85%)

(2) Individual data/application systems: — 17 (63%)

6. COMPUTER SECURITY SUBDISCIPLINES SPECIFICALLY INCLUDED (Please "X" all requirement sets that are included in the policy document, to include requirements that may be enumerated in a separate document -- e.g. the computer security document requires personnel security or communications security actions set forth in a referenced, separate document):

a. Personnel Security: — 26 (96%)

b. Physical Security: — 27 (100%)

c. Communications Security: — 24 (89%)

d. Emanations Security: — 19 (70%)

e. Administrative/Procedural Security: — 26 (96%)

f. Hardware/Software Security: — 26 (96%)

7. PROGRAM COMPONENT ELEMENTS (Please "X" all that are included in essence within the document):

a. Assignment of Responsibility:

(1) For computer security within the Agency or Department (i.e. specification of a headquarters staff element as responsible for policy promulgation and program oversight): 26 (96%)

(2) For specific ADP systems or ADP installations (e.g. Appointment of ADP System Security Officers): 25 (93%)

b. Management Control Process to assure that administrative, physical, technical and other safeguards are included in agency computer systems: 26 (96%)

c. Formally designated approving authority for the security aspects of covered ADP systems: 21 (78%)

d. Overall security specifications/requirements: 23 (85%)

e. Review, test and/or evaluation required as basis for system approval for operation: 20 (74%)

f. Audit or other follow-up system or program security evaluations: 21 (78%)

g. Risk Analysis or Risk Assessment methodologies 19 (70%)

h. Security Requirements/Specifications Applicable to Procurement (i.e. equipment, systems or related services): 20 (74%)

i. Requirements for Contingency Planning: 18 (67%)

j. Personnel Screening Requirements 21 (78%)

k. Specification of an authority to grant waivers: 15 (56%)

l. Requirement to specify an ADP security budget: 4 (15%)

SURVEY

EXECUTIVE BRANCH COMPUTER SECURITY POLICY DOCUMENTS

SUMMARY -- NATIONAL LEVEL

--Total documents: 13

--Total questionnaires: 5

--Total pages: 128

4. APPLICABILITY OF POLICY (Please "X" all that apply):

a. Applies to the department/agency identified in 1., above, and its components and facilities: 5 (100%)

b. Applies to all (or most) department/agency contractors (i.e. any industrial, educational, commercial or other entity which has executed a contract with the department/agency): 5 (100%)

5. PROTECTION SCOPE (Please "X" all that are included within the policy document):

a. Information/data

(1) Classified National Security Information: 4 (80%)
and/or
Unclassified "National Security Related Information:" 1 (20%)

(2) Personal information relating to individuals ("Privacy"): 3 (60%)

(3) Other agency/department "sensitive information" and records: 2 (40%)

b. (1) ADP systems (i.e. "Automatic Data Processing equipment," including computers and auxiliary or accessorial equipment such as I/O devices and communications equipment): 5 (100%)

(2) Areas housing ADP systems or their components (e.g. physical areas containing main frame or remote terminals): 4 (80%)

(3) Computer Programs (i.e. software) 4 (80%)

(4) Other ADP resources and supplies: 3 (60%)

c. Does the policy generally contain security requirements pertaining to the entire life cycle of ("X" if answer is "yes"):

(1) The ADP or computer systems concerned: 4 (80%)

(2) Individual data/application systems: 4 (80%)

6. COMPUTER SECURITY SUBDISCIPLINES SPECIFICALLY INCLUDED (Please "X" all requirement sets that are included in the policy document, to include requirements that may be enumerated in a separate document -- e.g. the computer security document requires personnel security or communications security actions set forth in a referenced, separate document):

a. Personnel Security: 4 (80%)

b. Physical Security: 5 (100%)

c. Communications Security: 5 (100%)

d. Emanations Security: 3 (60%)

e. Administrative/Procedural Security: 5 (100%)

f. Hardware/Software Security: 5 (100%)

7. PROGRAM COMPONENT ELEMENTS (Please "X" all that are included in essence within the document):

a.	Assignment of Responsibility:	
	(1) For computer security within the Agency or Department (i.e. specification of a headquarters staff element as responsible for policy promulgation and program oversight):	5 (100%)
	(2) For specific ADP systems or ADP installations (e.g. Appointment of ADP System Security Officers):	4 (80%)
b.	Management Control Process to assure that administrative, physical, technical and other safeguards are included in agency computer systems:	5 (100%)
c.	Formally designated approving authority for the security aspects of covered ADP systems:	4 (80%)
d.	Overall security specifications/requirements:	5 (100%)
e.	Review, test and/or evaluation required as basis for system approval for operation:	4 (80%)
f.	Audit or other follow-up system or program security evaluations:	4 (80%)
g.	Risk Analysis or Risk Assessment methodologies	3 (60%)
h.	Security Requirements/Specifications Applicable to Procurement (i.e. equipment, systems or related services):	3 (60%)
i.	Requirements for Contingency Planning:	1 (20%)
j.	Personnel Screening Requirements	4 (80%)
k.	Specification of an authority to grant waivers:	4 (80%)
l.	Requirement to specify an ADP security budget:	1 (20%)

January 1979

AGENCY COMPUTER SECURITY PROGRAM CHECKLIST

Use: To determine whether agency security programs conform to the requirements of OMB Circular No. A-71, Transmittal Memorandum No. 1 dated July 27, 1978.

Agency: _____.

Date of Plan(s): _____.

ASSIGNMENT OF RESPONSIBILITY FOR COMPUTER SECURITY

( ) Has the agency identified the individual having lead responsibility for computer security?

- Name of Individual _____.
- Title _____.
- Mailing Address _____.
- Phone Number _____.

( ) Has the agency assigned responsibility for computer security at each headquarters and field organization?

( ) Have the names and titles of individuals responsible for computer security at each facility/installation been identified?

( ) Do the individuals assigned responsibility for computer security have both computer and security experience?

( ) Has responsibility for computer security been formally assigned?

- By delegation memo? _____
- By job description? _____
- By charter statement? _____
- Other? _____

MANAGEMENT CONTROL PROCESS FOR COMPUTER APPLICATIONS

( ) Has the agency described a management control process to assure that appropriate administrative, physical and technical safeguards are built into all computer systems?

( ) Has the management control process been formally promulgated?

( ) Does the process allow for evaluation of the sensitivity of each current and new computer application?

- Does the process define the relative roles of the user, developer and operator of systems in determining the sensitivity of systems?
- Who makes the final system sensitivity determination?

SECURITY SPECIFICATIONS

( ) Does the agency management control process provide for defining and approving security specifications prior to programming new applications or making significant changes to old applications?

( ) Does the security specification development and approval process provide for consideration of the views of the user, the developer, the service organization, the individual assigned responsibility for computer security, and agency audit staff?

( ) Does the process define "significant changes to existing systems" and establish procedures for approval of security provisions prior to making changes to existing systems?

( ) Does the plan identify a date by when a review of security specifications for existing systems will be completed? Dates by when corrective action will be completed?

( ) Is the final authority for approving computer system security specifications clearly defined and formally established?

- Who makes the decision?_____

( ) Do the procedures assure that provisions of the approved security specifications are incorporated in agency administrative procedures and programming specifications?

- Who is responsible for follow-up?_____

DESIGN REVIEW PROCESS

( ) Do the agency procedures establish requirements and responsibilities for conducting design reviews?

( ) Does the design review process provide checks and balances to assure adherence to the approved security specification?

( ) Does the procedure provide for documenting design review results?

( ) Is the responsibility for approving system designs subsequent to design reviews established?

- Who approves?_____

SYSTEM TEST PROCESS

( ) Do the agency procedures establish requirements and responsibilities for conducting and approving systems tests?

( ) Are the relationships between the design review process and system test processes established?

( ) Do the agency's system test procedures require testing of all aspects of security -- including administrative procedures, financial checks and balances, physical security and technological security features?

( ) Are the results of previous audits considered in the test procedures?

( ) Does the procedure provide for documenting system test results?

( ) Are responsibilities for conducting system tests established?

- Who is responsible?_____

SYSTEM CERTIFICATION PROCESS

( ) Does the agency management control process preclude operation of any new or modified system prior to satisfactory completion of systems tests?

( ) Do the certification procedures assure conformance to approved security specifications?

( ) Do the certification procedures assure that all applicable Federal policies, regulations, and standards have been complied with?

( ) Do the procedures provide for periodic recertification of systems?

( ) Do the procedures provide for certification of all current operational systems?

- When will they be completed?

( ) Does the agency program define policies, criteria, and timetables for periodic recertification of systems?

( ) Are responsibilities for certification and recertification of systems established?

- Who is responsible?_____

AUDIT/EVALUATION REQUIREMENTS

( ) Does the agency programs make a distinction between security audits and security evaluations?

( ) Have audit requirements been formally established?

- Who is responsible?_____

( ) Have evaluation requirements been formally established?

- Who is responsible for the evaluation program?
- What organizations will participate in the security evaluation process?

( ) If agency program includes both audits and evaluations -- has a coordination mechanism been established between audit and evaluation groups?

- Who is responsible?_____.

( ) Has a master audit/evaluation schedule been prepared?

- Have criteria been established for determining the priority of audits/evaluations?

- Are high risk or highly sensitive applications identified?
- Have timetables been established for conducting audits/evaluations of all sensitive applications established?
- Is the interval for periodic audits/evaluations equal or less than three years?

( ) Is the audit or evaluation performed by an organization independent of the user and computer facility manager?

( ) Have computer audit and/or evaluation guidelines been established?

( ) Where applicable, are computer system audit requirements included in agency IG implementation plans?

( ) Are the documented system security specifications, design review results, system test results, and system certifications made available to the audit and evaluation staffs?

( ) Has the agency established an information system audit/evaluation training program?

( ) Does the audit/evaluation function include

- Examination of data sensitivity?
- Verification and validation of the adequacy of physical, administrative, financial, and technical control?
- Adequacy of security administration?

RISK ANALYSIS PROCESS

( ) Has the agency assigned responsibility for conducting periodic risk analyses?

- Who is responsible?_____.

( ) Does the risk analysis adequately measure the vulnerabilities at the installation?

- Related to the potential for fraud or theft?

- Related to the potential for inadvertant error or improper disclosure of information?
- Related to the potential financial risk?
- Related to the potential of causing harm to individuals or infringing on their rights of privacy?
- Related to the protection of proprietary data and potential harm to business?

( ) Has the relationship between the organization responsible for conducting risk analyses and other organizational elements been defined?

- Relationship to IG function?
- Relationship to audit function?
- Relationship to evaluation function?
- Relationship to inspections function?
- Relationship to security function?
- Relationship to program office?
- Relationship to computer operational function?

( ) Are requirements established for the conduct of risk analyses for government-owned-contractor-operated (GOCO) facilities as well as government operated facilities?

( ) Does the agency program include provisions for assessing risks related to computer services provided by other agencies and those provided through commercial services?

( ) GSA only - Have provisions been made to assess risks of government-wide services provided to agencies by or through GSA, to advise agencies of the level of security provided by those services?

( ) Where applicable, are the requirements for computer risk analyses included in agency vulnerability assessment plans being developed to implement the I.G. legislation?

( ) Has a specific timetable for conducting risk analyses been established?

- Is the interval between risk analyses commensurate with the sensitivity of the information processed?
- Is the interval between risk analyses less than five years?

( ) Where sensitive applications represent only a small portion of the workload of a particular computer, has consideration been given to moving the applications to a secure installation and avoiding the need to secure the complete installation for a small portion of its workload?

( ) Do the agency procedures require that a risk analysis be performed:

- Prior to the approval of design specifications for computer installations?
- Whenever there is a "significant change" to the physical facility, hardware or operating system software?

( ) Has the agency defined "significant change"?

( ) Is the definition of "significant change" commensurate with the sensitivity of the information processed by the installation?

( ) Are NBS draft guidelines on conducting risk assessments included in agency guidance?

PROCUREMENT REQUIREMENTS

( ) Have agency policies and procedures been established to assure that security requirements are included in specifications for:

- Equipment?
- Computer processing services?
- Facility management services?
- General purpose software?

- ° Operating system software?
- ° Design or programming of applications?

( ) Are the specifications reviewed by the security official to verify that:

- ° They are reasonably sufficient for the intended application.
- ° That they comply with current Federal computer security policies, procedures, standards and guidelines.

( ) Have the requirements been incorporated in the agency procurement policies and regulations?

( ) Do the procedures require review of the adequacy and security provisions in current contracts, consider the feasibility of renegotiating existing contracts where appropriate, or modifying the terms of existing contracts prior to renewing the contracts or exercising any extension options under the contracts?

( ) Has responsibility for these matters been assigned?

- ° To whom?_____

CONTINGENCY PLANS

( ) Has the agency established policies and responsibilities to assure that contingency plans (in the event of natural disaster, hardware/software failure, or any events which could cause a significant description of service) are developed and maintained?

( ) Are the contingency and back-up requirements established by the agency commensurate with the risk and magnitude of potential loss?

( ) Are the contingency plans reviewed and tested at periodic intervals? What intervals?_____

( ) Are the test intervals commensurate with the risk and magnitude of potential loss?

PERSONNEL SCREENING REQUIREMENTS

( ) Has the agency established personnel security policies for screening individuals?

( ) Does the personnel policy provide for levels of screening commensurate with the sensitivity of the function?

( ) Do the agency policies and criteria consider separation of duties in sensitive processes so that each position would be less sensitive?

( ) Have screening requirements for contractor personnel been established and implemented?

( ) Are the personnel policies consistent with FPM letter 732-7?

RESOURCE ESTIMATES ($ in thousands)

One-time Costs. Staff-Years_____ $_____

On-going Costs. Staff-Years_____ $_____

GENERAL COMMENTS

_____

_____

_____

_____

_____

_____

REVIEWER: _____

DATE: _____

COMPUTER SECURITY

A list of policies, regulations, reports and other reference documents pertaining to the development of Federal computer security programs:

- To reduce fraud and waste.
- To protect personal, proprietary and other sensitive information.

Office of Management and Budget
Information Systems Policy Division
February 1979

OMB POLICIES

- OMB Circular No. A-71, Transmittal Memorandum No. 1, "Security of Federal automated information systems," July 27, 1978 (Copy attached).

  - Agency Computer Security Program Checklist, January 1979 (Copy attached)

- OMB Circular No. A-108 as amended, "Responsibilities for the maintenance of records about individuals by Federal agencies," July 1975.

FEDERAL PERSONNEL MANUAL REQUIREMENTS

- FPM letter 732-7 "Personnel Security Program for Positions Associated with Federal Computer Systems," November 14, 1978.

FEDERAL PROCUREMENT REGULATIONS

- FPR 1-4.11 "Procurement and Contracting for Government-wide Automatic Data Processing Equipment, Software Maintenance Services, and Supplies," September 1976.

- FPR 1-1.327 "Protection of the Privacy of Individuals," September 1975.

FEDERAL PROPERTY MANAGEMENT REGULATIONS

- FPMR 101-36.7 "Management and Control of Computer Rooms and Related Support Areas," June 15, 1978.

- FPMR 101-35.17 "Privacy and Data Security for ADP and Telecommunications Systems," June 16, 1978.

- FPMR 101-20 "Management of Buildings and Grounds," June 16, 1978.

- FPMR 101-34 "Emergency Preparedness Planning," June 16, 1978.

- FPMR 101-37.6 "Essential Telephone Services During Emergencies," June 16, 1978.

STANDARDS

- FIPS PUB 46 "Data Encryption Standards," January 15, 1977.

GUIDELINES

- FIPS PUB 31 "Guidelines for ADP Physical Security and Risk Management," June 1974.
- FIPS PUB 39 "Glossary for Computer Systems Security," February 15, 1976.
- FIPS PUB 41 "Computer Security Guidelines for Implementing the Privacy Act of 1974," May 30, 1975.
- FIPS PUB 48 "Evaluation of Techniques for Automated Personal Identification," April 1, 1977.
- "Standard Practice for the Fire Protection of Essential Electronic Equipment Operations" published by the National Fire Prevention and Control Administration of the Department of Commerce, August 1978.

GAO REPORTS - which identify computer system design and security problems.

- FGMSD-76-5 "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government," April 23, 1976.
- FGMSD-76-27 "Computer-Related Crimes in Federal Programs," April 27, 1976.
- FGMSD-76-40 "Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities," May 10, 1976.
- FGMSD-77-32 "Computer Auditing in the Executive Departments: Not Enough is Being Done," September 28, 1977.
- FGMSD-77-14 "Problems Found with Government Acquisition and Use of Computers from November 1965 to December 1976," March 15, 1977
- LCD-77-102 "Vulnerabilities of Telecommunications Systems to Unauthorized Use," March 31, 1977.
- FGMSD-76-82 "New Methods Needed for Checking Payments Made by Computers," November 11, 1977.
- FPCD-77-64 "Proposals to Resolve Longstanding Problems in Investigations of Federal Employees," December 16, 1977
- LCD 76-102 "Challenges of Protecting Personal Information in an Expanding Federal Computer Environment," April 28, 1978.

- LCD-76-115 "Safeguarding Taxpayer Information--An Evaluation of the Proposed Computerized Tax Administration System," January 17, 1977.

- HRD-78-116 "Procedures to Safeguard Social Security Beneficiary Records Can and Should be Improved," June 5, 1978.

- FGMSD-78-27 "Inadequacies in Data Processing Planning in the Department of Commerce," May 1, 1978.

- CED-78-84 "Problems Persist in the Puerto Rico Food Stamp Program, The Nation's Largest," April 27, 1978.

- HRD-77-110 "Privacy Issues and Supplemental Security Income Benefits," November 5, 1977.

- LCD-78-123 "Automated Systems Security -- Federal Agencies Should Strengthen Safeguards Over Personal And Other Sensitive Data," January 23, 1979.

REFERENCE DOCUMENTS

- Senate Governmental Affairs Committee Print - "Problems Associated with Computer Technology in Federal Programs and Private Industry," June 21, 1976.

- Senate Governmental Affairs Committee Print - "Computer Security in Federal Programs," February 1977.

- The Report of the Privacy Protection Study Commission - "Personal Privacy in an Information Society," July 1977.

- "Report of the Commission on Federal Paperwork, Final Summary Report," October 3, 1977; and "Confidentiality and Privacy," June 29, 1977.

- "Computer Security Publications" published by the Institute for Computer Sciences and Technology of the National Bureau of Standards, July 1978.

EXTRACTS FROM:

AUDIT REPORT

SUMMARY REPORT ON THE AUDIT OF

ADP SYSTEMS SECURITY AND PRIVACY AT

SELECTED DEFENSE DATA PROCESSING INSTALLATIONS

DEFENSE AUDIT SERVICE

"Serving Management"

AUDIT REPORT NO. 952

DATE SEPTEMBER 29, 1978

APPENDIX G

ACTIVITIES INCLUDED IN THE AUDIT

Department of Defense

Office of Civilian Health and Medical Program
for the Uniformed Services, Denver, CO

Defense Agencies

Defense Communications Agency

Defense Commercial Communications Office, Scott Air Force
Base, IL

Defense Logistics Agency

Defense Depot, Ogden, UT
Defense Personnel Support Center, Philadelphia, PA
Defense Logistics Agency Administrative Support Center,
Cameron Station, Alexandria, VA
Defense Contract Administration Services Region, Atlanta, GA

Defense Nuclear Agency

Headquarters, Alexandria, VA
Armed Forces Radiobiology Research Institute, Bethesda, MD

Department of the Army

Headquarters

Army Automation Directorate, Office of the Chief of Staff,
Army, Washington, D.C.
Office of the Assistant Chief of Staff for Intelligence,
Washington, D.C.

Central Design Activities

US Army Computer Systems Command, Ft Belvoir, VA
Automated Logistics Management Systems Agency, Fort Lee, VA
US Army Finance and Accounting Center, Indianapolis, IN
US Army Management Systems Support Agency, Washington, D.C.

Data Processing Installations

US Army Military Personnel Center, Europe, Heidelberg, Germany
21st Support Command, Zweibruecken, Germany
US Army Management Systems Support Agency, Washington, D.C.
US Army Military Personnel Center, Alexandria, VA
US Army Forces Command, Fort McPherson, GA
XVIII Airborne Corps and Fort Bragg, Fort Bragg, NC
US Army Finance and Accounting Center, Indianapolis, IN
US Army Troop Support Command, St. Louis, MO
US Army Reserve Components Personnel and Administration Center,
St. Louis, MO

Department of the Navy

Aviation Supply Office, Philadelphia, PA
Data Processing Service Center Pacific, Alameda, CA
Fleet Material Support Office, Mechanicsburg, PA
Mare Island Naval Shipyard, Vallejo, CA
Naval Supply Center, Oakland, CA
Naval Air Test Center, Patuxent River, MD
Ships Parts Control Center, Mechanicsburg, PA

ACTIVITIES INCLUDED IN THE AUDIT

Department of the Air Force

Aerospace Defense Command

Peterson Air Force Base, CO

Air Force Logistics Command

Headquarters, Wright-Patterson Air Force Base, OH
McClellan Air Force Base, CA
Robins Air Force Base, GA

Air Training Command

Keesler Air Force Base, MS
Lackland Air Force Base, TX
Sheppard Air Force Base, TX

Air Force Systems Command

Aeronautical Systems Division, Wright-Patterson Air Force Base, OH
Edwards Air Force Base, CA

Military Airlift Command

Headquarters, Scott Air Force Base, IL
McGuire Air Force Base, NJ
Travis Air Force Base, CA

Strategic Air Command

Anderson Air Force Base, Guam
Beale Air Force Base, CA
Plattsburg Air Force Base, NY

Tactical Air Command

Headquarters, Langley Air Force Base, VA
Sargstrom Air Force Base, TX
MacDill Air Force Base, FL

United States Air Forces in Europe

Headquarters USAFE, Ramstein Air Base, Germany
Ramstein Air Base, Germany
Torrejon Air Base, Spain

Pacific Air Forces

Osan Air Base, Korea

Air National Guard

Air National Guard, Tucson, AZ
Buckley Field, CO
Cannelly Field, AL
Pease Air Force Base, NH
Will Rogers International Airport, OK

Air Force Accounting and Finance Center, Denver, CO
Air Force Data Systems Design Center, Gunter Air Force Base, Montgomery, AL

AD-A103 676 OFFICE OF THE SECRETARY OF DEFENSE WASHINGTON DC F/G 9/2
SURVEY OF FEDERAL COMPUTER SECURITY POLICIES,(U)
NOV 80 E V EPPERLY

UNCLASSIFIED NL

2 OF 2

END
DATE FILMED
10 81
DTIC

REPORTS ISSUED

	Report	
Defense Audit Service	Number	Date
Report on the Audit of ADP Systems Security and Privacy at the Defense Commercial Communications Office	838	Dec 6, 1977
Report on the Audit of ADP Systems Security and Privacy at Selected Defense Logistics Agency Activities	852	Feb 7, 1978
Report on the Audit of ADP Systems Security and Privacy at Selected Defense Nuclear Agency Activities	862	Mar 7, 1978
Report on the Audit of ADP Systems Security and Privacy at the Office of the Civilian Health and Medical Program for the Uniformed Services	873	Mar 28, 1978
Army Audit Agency		
Report of Audit, System Security and Privacy at Data Processing Installations	EC 77-219	Aug 31, 1977
Naval Audit Service		
Audit Survey Report, Security Considerations in Automatic Data Processing Systems Preventing Fraud in Supply Operations	I20086	Nov 23, 1977
Air Force Audit Agency		
Interservice Audit of Computer Systems Security and Privacy	SRA 75333	Dec 21, 1977

PROPOSED DOD SENSITIVITY CATEGORIES

Sensitivity Categories -- Data & Applications (Figure 1)
ADP I, "Critical-Sensitive". DoD data and applications stored or processed in, or communicated, displayed or disseminated by, an Automatic Data Processing (ADP) System shall be categorized as ADP I when one or more of the following criteria are met:

- Top Secret National Security Information -- The data or applications require protection in the interest of national security, and the classification designation is "Top Secret" (DoD Regulation 5200.1-R);

- Mission Critical -- The data or applications are such that the denial of use, loss, compromise, disablement or unauthorized alteration thereof could reasonably be expected to directly and gravely degrade or

DATA & APPLICATIONS

CAT I:

- TOP SECRET
- MISSION
- LIFE
- $10 M/YR.

CAT II:

- SECRET & CONF
- MISSION
- PRIVACY
- FOIA
- $1 - 10 M/YR.

CAT III:

- ALL OTHERS

Figure 1

ADP SYSTEMS

CAT I:

- CAT I DATA/APPLICATION

CAT II:

- CAT II DATA/APPL.

CAT III:

- ALL OTHERS

Figure 2

jeopardize the capabilities of a Military Department, the Joint Chiefs of Staff, a Defense Agency or a Unified or Specified Command to timely and effective discharge of their primary functions (DoD Directive 5100.1) in support of DoD emergency and/or war plans;

- Life Critical -- The data or applications are such that the denial of use, loss, compromise, disablement or unauthorized alteration thereof could reasonably be expected to directly and gravely jeopardize human life;

- Automated Decisionmaking Systems -- Applications, not otherwise included in the foregoing, which issue checks, requisition supplies or perform similar assets control functions, based on programmed criteria with little human intervention, wherein the potential loss or exploitable monetary value of the assets handled could exceed $10,000,000 per year.

ADP II, "Noncritical-Sensitive". DoD data and applications, which do not meet any of the foregoing criteria for category ADP I, shall be categorized as ADP II when one or more of the following criteria are met:

- Secret or Confidential National Security Information -- The data or applications require protection in the interest of national security, and the classification designation is either "Secret" or "Confidential" (DoD Regulation 5200.1-R);

- Mission Critical -- The data or applications are such that the denial of use, loss, compromise, disablement or unauthorized alteration thereof could reasonably be expected to degrade or jeopardize component command or major staff element capabilities to support timely and effective discharge of Military Department, OJCS, Defense Agency or U & S Command missions and functions;

- Privacy -- The data or applications involve personal information requiring protection pursuant to the Privacy Act of 1974 (DoD Directive 5400.7);

- FOIA Exemptions -- The data or applications (unclassified) have been determined to be exempt from public disclosure, consistent with the requirements of the Freedom of Information Act (FOIA) (Section VI, DoD Directive 5400.7);

- Automated Decisionmaking Systems -- Applications, not otherwise included in the foregoing, which issue checks, requisition supplies or perform similar assets control functions, based on programmed criteria with little human intervention, wherein the potential loss or exploitable monetary value of the assets handled could range between $1,000,000 and $10,000,000 per year.

ADP III, "Nonsensitive". All other DoD data and applications which do not meet the criteria for categories ADP I or ADP II as set forth above.

Sensitivity Categories -- ADP Systems (Figure 2)

ADP I, "Critical-Sensitive". ADP systems shall be categorized as ADP I when either of the following criteria is met:

- ADP I Data or Applications -- The ADP system stores or processes one or more sets of data or applications categorized as ADP I, "Critical-Sensitive," pursuant to the criteria herein; or,

- Automated Decisionmaking Systems -- The ADP system handles "automated decisionmaking systems" wherein the aggregate total potential loss or exploitable monetary value of assets handled collectively by the ADP system's automated decisonmaking systems applications could exceed $10,000,000 per year.

ADP II, "Noncritical-Sensitive". ADP systems, which do not meet any of the foregoing criteria for category ADP I, shall be categorized as ADP II when either of the following criteria is met:

- ADP II Data or Applications -- The ADP system stores or processes one or more sets of data or applications categorized as ADP I; or,

- Automated Decisionmaking Systems -- The ADP system handles "automated decisionmaking systems" wherein the aggregate total potential loss or exploitable monetary value of assets handled collectively by the ADP system's automated decisionmaking systems applications could fall between $1,000,000 and $10,000,000 per year.

ADP III, "Nonsensitive". All other ADP systems processing DoD data or applications.

Sensitivity Categories -- Personnel Positions (Figure 3)

ADP I, "Critical-Sensitive". Positions of personnel requiring access to ADP I DoD data or applications OR unescorted access to an ADP I ADP system(s).

ADP II, "Noncritical-Sensitive". Positions of personnel requiring access to ADP II DoD data or applications OR unescorted access to an ADP II ADP system(s).

ADP III, "Nonsensitive". Positions of all other personnel requiring access to DoD data or applications OR requiring unescorted access to an ADP system containing DoD data or applications.

Now when we link the foregoing to the system security mode concepts already presented, we have the capability to minimize personnel security clearances for systems, based, in the terms of this seminar, on the relative "trustedness" of the internal system security controls. For example:

POSITIONS

CAT I – REQUIRED ACCESS TO: CAT I DATA/APPL OR SYSTEMS

CAT II – REQUIRED ACCESS TO: CAT II DATA/APPL OR SYSTEMS

CAT III – ALL OTHERS

Figure 3

ADJUSTMENTS

– TEMPORARY DEDICATION

– "MLS & CONTROLLED MODE"

– OUTPUT ONLY

– "TECHNICAL REVIEW"

Figure 4

Adjustments for Position Sensitivity Categories (Figure 4)

1. "Multilevel and Controlled Mode" Systems -- The positions of ADP System Users with access to systems already approved to operate in either the "Controlled Security Mode" or the "Multilevel Security Mode" pursuant to DoD Directive 5200.28 (or, for contractor ADP systems, DoD Manual 5220.22-M) shall be designated in the position sensitivity category commensurate with the most sensitive category of the DoD data or application(s) they will access under system constraints.

2. "Temporarily Dedicated" Systems -- The positions of personnel with access to ADP systems currently operating under procedures that effect temporary dedication to different sensitivity categories at different periods of time (also called "color changing" or "periods processing") shall be designated in the sensitivity category commensurate with the most sensitive category of DoD data or application(s) contained in the system during periods of each individual's access to the system. In remotely accessed systems, this will include remote terminal users wherein the remote terminal is disconnected during higher sensitivity category processing periods.

3. "Output Only" -- The positions of ADP System User personnel shall be designated in the position sensitivity category commensurate with the category of only the system output they actually receive when: (1) such personnel do not input to or otherwise directly interact with the system (i.e., no "hands on" or other direct input or inquiry capability), and (2) the output products are either reviewed prior to dissemination or otherwise determined to be properly identified as to content, intended recipient and sensitivity category (i.e., systems approved to implement this option pursuant to paragraph IV.C.5.b., DoD Directive 5200.28 or for contractor ADP systems, paragraph 108, DoD Manual 5220.22-M).

4. "Technical Review" -- The positions of personnel who design, develop or generate DoD data or applications, or who generate input to an ADP system containing DoD data or applications, shall be designated in a less sensitive position category when (1) such personnel do not have access to ADP systems containing higher sensitivity category data or applications, and (2) when the product or input generated by such personnel is subject to "Technical Review."

The most important consequence of the foregoing is that if we pursue this concept then the need for "trusted" systems, just within Defense, will expand from potentially 27% of our inventory (the subset that processes classified information) of general purpose ADP systems to 100%. With Defense contractors, the requirement is expected to also increase, although there is no basis for anticipating specific numbers.

23 JAN 1979

COMPTROLLER GENERAL'S
REPORT TO THE CONGRESS

AUTOMATED SYSTEMS SECURITY--FEDERAL AGENCIES SHOULD STRENGTHEN SAFEGUARDS OVER PERSONAL AND OTHER SENSITIVE DATA

D I G E S T

Federal agencies GAO surveyed did not have a centrally directed program to protect effectively personal and other sensitive data in computer systems. Programs fell short of being comprehensive and top management support was lacking. This was, in part, because upper management either did not recognize or adequately appreciate their responsibilities in this area or recognize the potential for invading the privacy of people or organizations served by the agency and for damage to agency program operations.

GAO surveyed selected agencies in 1977 because of the generally high level of congressional interest in Federal information policies following the enactment of the Privacy Act and the Freedom of Information Act Amendments in 1974. Subsequently, GAO was specifically requested to examine and report on the status and effectiveness of major Federal agencies' computer security programs by the Chairman of the House Subcommittee on Government Information and Individual Rights, House Committee on Government Operations. (See p. 1.)

GAO's review included 10 civil agencies but excluded the highly specialized area of controls over national security classified data in Defense agencies. (See p. 2.) Many other agencies throughout the Government are experiencing to varying degrees some of the same weaknesses. In fact, GAO's review further confirmed automated system security and control problems disclosed in many prior GAO published reports. (See p. 3.)

LCD-78-123

APPENDIX I

In a larger sense, these findings have potential applicability wherever computers are used intensively. This is because of the pervasiveness of the underlying causes of poor data security. Modern computer based information systems represent relatively recent technology that has introduced many new threats adding to management problems of maintaining data at acceptable levels of integrity and security. (See pp. 7 and 8.)

WEAKNESSES IN AGENCY PROGRAMS FOR COMPUTER SECURITY

GAO focused on weaknesses in the agencies' systems of management controls, including appropriate organizations, monitoring and reporting, use of risk analysis, and use of independent internal audits. (See pp. 10 27, and 47.)

Particular attention was given to the degree of agencies' efforts to organize and implement broadly conceived programs of data security in compliance with the Office of Management and Budget (OMB) directives and related computer security guidance published by the National Bureau of Standards, Department of Commerce. (See p. 10.)

Although all agencies reviewed had some elements of a computer security program in varying stages of being, they lacked the management support needed to be truly comprehensive. (See p. 10.)

Security programs usually were not developed from the perspective of the total data system; consequently, any weak link could result in ineffective security. For example, the scope of most security programs did not cover data in all media and in all stages of the data life cycle nor did they consider all possible threats at all locations involved with the agencies' data. Additionally, many programs did not have written plans, policies, and procedures. (See p. 11.)

Also, management generally did not place the computer security function at a sufficiently high level, with independence from operating functions, to preclude preemption by operational priorities. Thus, authority to recommend and enforce security measures was seriously lacking. Agencies did not establish clear responsibilities of individuals and organizations. (See p. 14.)

Management generally was giving inadequate attention to monitoring the aspects of computer security in their organizations to be sufficiently informed on how their security measures were working. Management was not receiving the feedback necessary for control of computer data security. (See p. 20.)

Agencies usually had selected computer systems safeguards intuitively rather than on a cost-effectiveness determination which would take into account the degree of sensitivity and vulnerability of the information to be protected. This risk management concept, which should be applied in all determinations to select economically feasible safeguards considering the particular environment where the data is processed, was generally not employed. (See p. 27.)

Security programs should but usually did not address all of the necessary elements of technical, administrative, and physical safeguards. In many cases, attention had been given by technicians and lower and middle level managers to the obvious and traditional safeguards. However, safeguard protection that required upper level management and administration were neglected. (See p. 30.)

INTERNAL AUDIT

At a time of increasing reliance on computers and rapidly advancing automated data processing technology, internal audit can be a

vital resource for keeping management informed on data security requirements and how well these responsibilities are being met. However, at the agencies surveyed, independent internal audit generally was not significantly involved in assessing computer based systems controls or conducting more conventional security compliance audits.

Agency internal audit was not significantly involved in computer security because of a lack of technical expertise. Discussions with Internal Audit officials revealed that the expertise needed to challenge security shortcomings has not been developed because top management has not tasked internal audit in a computer security role. (See p. 47.)

OMB's GUIDANCE TO AGENCIES

Although OMB has stressed that data security and integrity are the responsibilities of the heads of departments and agencies, GAO found that agencies did not take the initiative to meet these responsibilities.

OMB's policy guidance and technical guidance provided by the National Bureau of Standards was largely ignored and not used to advantage. Consequently, the agency security programs did not reflect the intent of this guidance.

CONCLUSIONS

OMB issued Circular A-71, TM-1--on Security of Federal Automated Information Systems--after completion of this review. The circular requires action by agency top managers which could contribute greatly to correcting many of the computer data security problems addressed in the GAO report. The circular is directive. It is also quite comprehensive. It requires agency heads to report on their plans to to comply. (See p. 23.)

Specifically, the circular promulgates policies and responsibilities for the development and implementation of computer security programs by all executive departments and agencies: It further addresses the general requirement for agencies to implement a computer security program; it establishes specific requirements for the development of management controls to safeguard personal, proprietary and other sensitive data in automated systems; and it defines a minimum set of technical controls to be incorporated into each agency computer security program. (See app. IV.) Therefore, it sets an appropriate framework for agencies' initiatives to correct their data security problems.

RECOMMENDATION TO OMB

GAO views a leadership role by OMB as vital to maintaining the momentum that Circular A-71 should impart to computer security in Federal agencies. GAO is concerned that agencies may lose sight of the stated purpose of the directive, i.e., that agencies develop and implement computer security programs with a scope to protect personal, proprietary and other sensitive data. The circular further addresses certain specific technical requirements. Accordingly, GAO sees a critical need for OMB to follow up on the circular's requirement that agencies prepare and submit plans for compliance. (See p. 23.)

The Director of OMB should arrange for independent reviews by persons knowledgeable in computer security of the plans of departments and agencies responding to Circular A-71. OMB should critique agencies on the adequacy of their plans for computer security using the findings and recommendations to heads of agencies contained in this report as well as the requirements set forth in Circular A-71. (See p. 23.)

RECOMMENDATIONS TO HEADS OF FEDERAL AGENCIES

All agencies should strengthen their computer data security and integrity, highlighted as follows.

--Computer security programs should be comprehensive. They should include plans, policies, and procedures in writing that clearly establish responsibilities throughout the organization. (See p. 25.)

--Agencies should establish a computer security administration function with independence from computer operations. This organization should report directly to or through a principal official who reports directly to the agency head. (See p. 24.)

--Programs should provide for feedback for management control, both in routine monitoring and reporting and in independent internal audits. (See pp. 25 and 52.)

--Risk management should be provided for and should be on the perspective of the total data systems. (See p. 46.)

--Security planning should anticipate training needs, particularly for risk management. (See pp. 25, 46, and 52.)

OMB's COMMENTS

OMB representatives indicated that GAO's examination of the status and effectiveness of computer system security programs provided information and recommendations which would be used and followed up in their own assessments of Federal agencies' plans to comply with their Circular A-71 and other requirements.

OMB is placing a high priority on efforts over the coming year to improving security programs in agencies and has organized a task force to accomplish reviews of agencies' plans. This effort is coupled with OMB's broader concerns for improving controls in agencies over fraud and abuse. OMB indicated that attention by agencies' inspector general functions will be focused on correcting these matters in recognition that they are important responsibilities of agency and department heads.

OMB expressed some concern that GAO's recommendation for organizing a highly placed computer security administration as a staff function, independent from computer operations, might cause difficulty with the agency head's span of control. That is, too many functions are now competing for top-level attention and this would add one more. GAO intends its recommendation to be sufficiently broad to allow each agency maximum flexibility in its implementation in a wide variety of agency organizations.

GAO agrees with OMB that elements of this security function such as monitoring, inspection, and audit could be placed under the inspector general function. But GAO sees the need for identification of a focal point at a high level, independent from responsibility for computer operations, to develop and oversee an automated systems security program. The security program itself should be promulgated by a directive and guidance issued by the agency head. (See p. 24.)

END

DATE
FILMED
10-81

DTIC