1989 COMPUTER SECURITY AND PRIVACY PLANS (CSPP) REVIEW PROJECT: A FIRST-YEAR FEDERAL RESPONSE TO THE COMPUTER SECURITY ACT OF 1987 (FINAL REPORT)

Dennis M. Gilbert, Report Coordinator
National Computer Systems Laboratory

Jointly prepared by:
National Computer Systems Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

National Computer Security Center
National Security Agency
U.S. Department of Defense

NIST

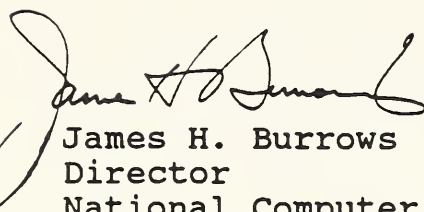# 1989 COMPUTER SECURITY AND PRIVACY PLANS (CSPP) REVIEW PROJECT: A FIRST-YEAR FEDERAL RESPONSE TO THE COMPUTER SECURITY ACT OF 1987 (FINAL REPORT)

Dennis M. Gilbert, Report Coordinator
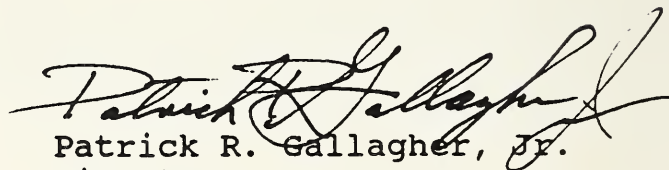National Computer Systems Laboratory

ABSTRACT

The goal of the Computer Security Act of 1987 (Public Law 100-235) (the Act) is to prompt federal agencies to take measures to improve the security and privacy of sensitive information in federal computer systems. The Act requires federal agencies to prepare and submit for review security plans for unclassified computer systems that contain sensitive information. The Act provides that the plans be submitted to the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) for review and comment. This report describes the Computer Security and Privacy Plan (CSPP) review effort that was conducted in response to the Act by a joint team from NIST and NSA in 1989. The report also discusses future directions for implementing the Act.

The Computer Security Act of 1987 (the Act) has further increased our growing awareness that information and information resources are integral to the functioning of government - and that their protection is fundamental, not peripheral to, the government serving the public trust. We applaud and support the efforts undertaken under the Act and welcome the opportunity to further serve in this area.

We would like to acknowledge, congratulate, and thank the many individuals and agencies that took the time and effort to seriously examine their computer security programs and plans. We are proud of the vital role that our organizations play in supporting the Act's goals. We look forward to continued cooperation between our organizations in carrying out the spirit of the Computer Security Act to better serve the federal community and, ultimately, the public.
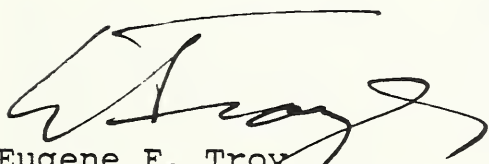
James H. Burrows
Director
National Computer
    Systems Laboratory
National Institute of
    Standards and Technology

Patrick R. Gallagher, Jr.
Director
National Computer
    Security Center
National Security
    Agency

iv

We appreciate the opportunity to participate in this historic chapter of promoting the protection of federal information and information technology resources. We take pride in the manner in which our organizations and staffs worked together and in what this project has started. We thank those who participated in this initial journey and who contributed to our collective learning about the challenges we face and how we address them.

Eugene F. Troy
CSPP Review Project
   Co-manager
National Institute of
   Standards and Technology

Christopher P. Bythewood, Jr.
CSPP Review Project
   Co-manager
National Security Agency

SUMMARY REPORT OF THE
COMPUTER SECURITY AND PRIVACY PLANS (CSPP) REVIEW PROJECT

PURPOSE

Sensitive information and information resources have become increasingly important to the functioning of the federal government. The protection of such information is integral to the government serving the public trust. Concern that federal agencies were not protecting their information caused Congress to enact Public Law 100-235, "Computer Security Act of 1987" (the Act). This document summarizes the report on the governmentwide computer security planning and review process required by the Act.

BACKGROUND

The Act reaffirmed the National Institute of Standards and Technology's (NIST) computer security responsibilities. These responsibilities include developing standards and guidelines to protect sensitive unclassified information. Other responsibilities include providing new governmentwide programs in computer security awareness training and security planning.

The Act required federal agencies to conduct educational programs to increase staff awareness of the need for computer security. The first-year activity included agencies identifying their computer systems containing sensitive information. These agencies prepared and submitted security plans for those systems to the NIST and National Security Agency (NSA) review team for advice and comment.
*

THE CSPP REVIEW PROJECT

The Office of Management and Budget (OMB) issued OMB Bulletin 88-16, "Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information," to guide agencies on preparing and submitting computer security plans. The bulletin specified the information that was to appear in each plan. The bulletin further requested that agencies identify systems as major application or general ADP support systems. Finally, the bulletin provided the agency the option of identifying any needs for guidance or technical support. This option also included making any comments the agency thought appropriate. Although a four-part format appeared, agencies were able to use latitude as long as all pertinent information was present. This permitted agencies with existing programs to submit current related

documents. Submission of an agency overview was optional and most agencies chose not to provide one.

The joint NIST/NSA review team examined 1,583 plans for 63 federal civilian agencies and 27,992 plans from 441 Department of Defense (DoD) organizations. Most DoD submissions consisted mainly of accreditation documentation prepared for other computer security planning purposes. During the review process, the review team recorded data about the systems for analysis. The conclusions made in this report stem principally, but not exclusively, from the civilian agency submissions.

MAJOR FINDINGS

The review team arrived at a number of conclusions about the plans and the plan review process, seeing both many positive signs and some areas for improvement. These findings include:

1)   The civilian agency CSPPs basically conformed with the guidance given by OMB Bulletin 88-16. Many controls to protect sensitive systems were already in place or planned. These controls appeared consistent with identified system functions, environment, and security needs. However, some respondents appeared to have just "checked the boxes," perhaps presenting a falsely optimistic picture.

2)   Many agencies appeared to report on isolated systems rather than all systems subject to the Computer Security Act and OMB Bulletin 88-16.

3)   Agencywide guidance on how to prepare the plans was not clear. There was also some question whether a high level official reviewed the plans. Also unclear is the distribution of agency-level computer security policy and guidance. Further, most plans did not reflect the joint involvement of ADP, computer security, and applications communities in computer security planning.

4)   Significantly, the plans rarely addressed the security concerns on networking, interfaces with other systems, and the use of contractors and their facilities. This may reflect a general confusion about the boundaries and limits of responsibility for a given system.

5)   Many plans equated sensitivity only with privacy or confidentiality, and did not fully address requirements for integrity and availability.

6) Most plans did not communicate an appreciation for the role of risk management activities in computer security planning.

7) Although most agencies said they had computer security awareness and training, many did not show that all applicable employees received periodic training.

8) Finally, the CSPP submission and review effort raised the level of federal awareness regarding the need to protect sensitive information and the importance of computer security planning.

RECOMMENDATIONS FOR AGENCIES

Based on the needs that became apparent during the plan review, the review team recommends the following:

1) Agency management should ensure that computer security has the highest level of management involvement. This involvement is also important in the computer security planning process. Computer security benefits from the multiple perspectives of and input from agency IRM, computer security, and functional, user, and applications personnel.

2) Agency management should identify and describe the security needs of their systems which contain sensitive information.

3) Agency management should recognize the importance of computer security and its required planning. This recognition should be aggressively communicated to their staffs, perhaps using their computer security and awareness training programs as one of the vehicles.

4) Agencies should incorporate computer security planning with other information systems planning activities.

5) Agencies should consider the protection requirements for integrity and availability on an equal basis with that of confidentiality.

6) Agencies should assess risks and select and implement realistic controls throughout the system life cycle. This involves awareness of technology changes with regard system hardware and software. This awareness also requires a knowledge of new technology and new methods for protecting and recovering from system threats.

Agencies also should fully document in-place controls to ease periodic reevaluation, internal audit, and oversight agency review.

7)   Agencies should implement certification and accreditation programs.   There is a lack of awareness of guidance regarding certification and accreditation, including FIPS PUB 102, "Guideline for Computer Security Certification and Accreditation."   There is also a lack of knowledge of the certification requirements in OMB Circular A-130, "Management of Federal Information Resources."   Agencies may use OMB Circular A-130 as the basis for these programs.

8)   Agencies should clarify the boundaries and limits of responsibility for each system, and should include, in any planned risk assessment activity, full consideration of the telecommunications and networking environment and relationships with contractors and other organizations.

9)   Agencies should stress security awareness and training for their employees.   This includes all employees involved in the design, management, development, operation, or use of federal computer systems containing sensitive information.

10)   Agencies should develop computer security policy and operative guidance.   Such policy and guidance should fully reflect and comprehensively address an encompassing view of computer security.   The Computer Security Act, OMB Circular A-130, and OMB Bulletins 88-16 and 89-17, "Federal Information Systems and Technology Planning," and their successors all contain this view.   The policy should directly address the full scope of computer security planning and risk management activities.   It must incorporate an application system perspective, and give more detailed consideration to confidentiality, integrity, and availability protection requirements.

NIST PLANS

NIST is evolving a strategy for helping federal agencies in identifying and protecting sensitive information systems.   This strategy shifts emphasis to the implementation of computer security plans, particularly those developed under OMB Bulletin 88-16.   It provides for visits by OMB, NIST, and NSA staff.   This group will provide direct comments, advice, and technical aid focused on the agency's implementation of the Act.

In addition to the agency visits described above, NIST has initiated the following computer security projects to help agencies more easily and effectively comply with the Computer Security Act:

1) NIST will develop standardized specifications and language for federal government computer security services contracts.

2) NIST will develop a guidance document on computer security in the ADP procurement cycle.

3) NIST has recently published guidance on the use of Trusted Systems.

4) NIST will develop guidance on computer security planning.

5) NIST has developed, and will continue to operate, a computer incident response center in order to address viruses, worms, and other malicious software attacks.

6) NIST will support and coordinate computer security resource and response centers nationwide.

7) NIST will enhance and operate the NCSL Computer Security Bulletin Board System.

8) NIST will operate the NIST/NSA Risk Management Laboratory and prepare further guidelines on risk management.

9) NIST will develop guidance and recommendations on assuring information integrity in computer systems.

In addition to the above plans, NIST has already developed a number of guidelines and other resources to help federal managers secure their computer systems. See Section VI.E, NIST Plans, of the full report for further details.

LESSONS AND BENEFITS

Federal managers have computer security requirements that are similar to their counterparts in the private sector. We believe that private sector organizations can learn and benefit from the federal experience in implementing the Computer Security Act. In both environments, a vigorous computer security awareness program is important at <u>all</u> levels in the organization. Also, in both environments, the active involvement of user, management, ADP, and computer security communities in computer security planning could help end some of the existing and potential barriers to effective computer security. Such collective involvement would also help

ensure cost-effective control measures commensurate with system
function, system sensitivity, security requirements, and analyzed
and considered risks.

SOME CLOSING THOUGHTS

Agencies need to be aware of developments taking place in the
national and international standards arena on system
interoperability and data interchange. These developments will
impact information system product availability, protection
requirements, and protection alternatives as agencies do their
near-, mid-, and long-term IRM and computer security planning.

Finally, because agency awareness of problems is fundamental to the
solution, this project has been valuable. Computer security
officers say that the CSPP preparation and review activity has
raised the level of awareness in all parts of their organizations
and has made it easier for them to promote computer security. The
CSPP review project significantly raised the level of federal
awareness about the protection of sensitive information and the
importance of computer security planning. In the final analysis,
this contribution may be among the most meaningful results of the
project.

PROJECT PARTICIPANTS

Christopher Bythewood
NSA, Project Manager

Eugene Troy
NIST, Project Manager

Douglas Hunt
NIST, Project Manager
(Former)

Jon Arneson, NIST, CSPP Review Team Leader
Gerald Everett, NSA, CSPP Review Team Leader
Dennis Gilbert, NIST, CSPP Review Team Leader
Barbara Guttman, NIST, Edit Team Leader
John Patrick, NSA, CSPP Review Team Leader
James Tippett, NSA, CSPP Review Team Leader

Robin Baker, NIST
Edward Borodkin, NSA
Annette Brooker-Grogan, NSA
Genevieve Cagney, NSA
Kathie Everhart, NIST
Ellen Flahavin, NIST
Gary Gambrell, NSA
James Gordon, NSA
Myrna Hodge, NSA
Victoria Howard, NIST
Leon Howell, NSA
Nickilyn Lynch, NIST
Victor Mathurin, NSA
Sam McCrea, NIST
John McCumber, NSA
Kathleen McKee, NSA
Darlene Nelson, NSA
Cinthia Olga, NSA
Wanda Perry, NSA
Lorrayne Schaffer, TIS
Raymond Shilinski, NSA
Diann Vechery, TIS
Dawn Wolcott, TIS

TIS - Trusted Information Systems, Inc.

ACKNOWLEDGEMENTS

REPORT CONTRIBUTORS

Edward Borodkin, NSA
Christopher Bythewood, NSA
Genevieve Cagney, NSA
Kathie Everhart, NIST
Dennis Gilbert, NIST
Barbara Guttman, NIST
Victoria Howard, NIST
Nickilyn Lynch, NIST
Raymond Shilinski, NSA
Eugene Troy, NIST

We would like to give special thanks to:

Robin Baker, Secretary of the Computer
Security Planning and Assistance Group, for
her outstanding help throughout the project.

Diann Vechery, Trusted Information Systems,
Inc. Project Leader, for her many significant
contributions to the project.

Those who prepared the Computer Security and
Privacy Plans, for their time and effort.

FINAL REPORT
1989 COMPUTER SECURITY AND PRIVACY PLANS (CSPP)
REVIEW PROJECT:
A FIRST-YEAR FEDERAL RESPONSE TO
THE COMPUTER SECURITY ACT OF 1987

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF FIGURES (CONTINUED)

LIST OF TABLES

LIST OF APPENDICES

I. INTRODUCTION

By establishing Public Law 100-235, "Computer Security Act of 1987" (the Act), Congress enacted a measure for establishing minimum acceptable security practices for federal computer systems that contain sensitive unclassified information. The goal of the Act is to prompt federal agencies to take measures to improve the security and privacy of these systems. The Act revises and expands the role of the National Institute of Standards and Technology (NIST, formerly the National Bureau of Standards, or NBS) in establishing and promulgating of standards and guidelines for unclassified computing, with the technical assistance of the National Security Agency (NSA). Additionally, the Act provides for the mandatory periodic computer security training for all persons involved in the management, use, and acquisition of sensitive federal systems. The Act also requires all federal agencies to prepare and submit security plans for all systems that contain sensitive unclassified data to NIST and NSA for advice and comment.

A.   Purpose and Scope of this Report

The purpose of this report is to provide insight into the initial implementation of the Act and the Computer Security and Privacy Plans (CSPP) Review Process, performed jointly by NIST and NSA in 1989. It includes the review team's findings, observations and analysis of the data collected from agency security plans, and some thoughts and comments on the process itself.

B.   The Computer Security Act and Related Guidance

The following two sections discuss the Computer Security Act and OMB Bulletin 88-16, "Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information," which provided first-year implementing instructions under the Act.

1.   The Computer Security Act of 1987

Concern about federal information resources and computer security is not new. Beginning with the Brooks Act of 1965 and the Paperwork Reduction Act of 1980, Congress attempted to address the growing role of computers in society. Major computer security milestones were the Counterfeit Access Device and Computer Fraud Act of 1984, and later the Computer Fraud and Abuse Act of 1986. These laws define activities determined to be contrary to the best interests of federal computing, in such areas as national security, financial integrity and management, and the privacy and confidentiality of information (as identified in the Privacy Act of 1974). Signed into law on January 8, 1988, the Computer Security Act further enhances the defense of federal systems that

contain sensitive information.

The Act represents a significant step in the federal government's increasing acceptance of responsibility to protect the confidentiality, integrity, and availability of its information systems and resources. It offers a means of fostering minimum acceptable security practices, without limiting the scope of security measures that are already planned or in use. Its goal is for federal agencies to take measures to improve the security of federal computer systems, with emphasis on computer security planning and on training and awareness. The Act deals with non-classified but sensitive federal systems, but excludes classified and intelligence-oriented systems.

Among its definitions, the Act defines "sensitive information" as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs or the privacy to which individuals are entitled under the Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy." (See Appendix A for the full text of the Act.)

Specifically, the Act requires each federal agency to: 1) identify each existing computer system, system under development, or systems under its supervision that contains sensitive information; 2) provide for the mandatory periodic training and awareness regarding accepted computer security practices for all employees involved in the management, use, or operation of each computer system under federal agency supervision; and 3) develop a plan to provide for the security and privacy of each federal computer system processing sensitive information. The plan needs to be commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system. The plans are to be submitted to NIST and NSA for advice and comment. The Act provided OMB with exclusive authority to disapprove the agency's plans. Additionally, the Act assigns to NIST the responsibility for developing standards and guidelines for the security and privacy of sensitive information in federal computer systems. Moreover, the Act establishes a Computer Security and Privacy Advisory Board to identify emerging federal computer and privacy issues.

2. OMB Bulletin 88-16

OMB Bulletin 88-16, "Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information," was issued to help federal agencies prepare their CSPPs. (Appendix C contains the text of the bulletin.) The

bulletin, prepared with the assistance of NIST and NSA, drew heavily on NIST computer security standards and guidance documents.

The bulletin specified that the following information be provided in each plan: 1) basic system identification, including "generic" types of information processed, "generic" types of processing, and a description of the system's environment; 2) sensitivity of information handled, including the reason(s) the system is considered sensitive, and the requirements for protecting it in terms of confidentiality, integrity, and availability; and 3) a description of security measures designed or planned to protect the system, including managerial, developmental, operational, and technical controls. The plans were to have indicated whether these control measures are in place, planned, or not applicable.

The bulletin further requested that systems be categorized as major application or general ADP support systems. Finally, the bulletin provided the agency the option of identifying any needs for guidance or technical support and to make any comments the agency deemed appropriate. Although a four-part format was indicated, agencies were permitted latitude as long as all pertinent information was present. This permitted agencies with existing programs to submit current related documents. Although submission of an agency overview was optional, most agencies chose not to provide one.

C.   CSPP Review Project Objectives

The primary objective of the Computer Security and Privacy Plan Review Project was to provide advice and comment on the CSPPs, the goal being to raise awareness of the importance of identifying and safeguarding sensitive information. A secondary objective was to obtain a better picture of the current state of computer security planning for systems containing sensitive information and to assess needed improvements.

D.   Document Overview

The following sections of this report detail the review project. Section II discusses the review team, the guide used by the review team, and the separate processes used to review the civilian and defense agencies' CSPPs. Section III analyzes the civilian agency and DoD submissions; Sections IV and V report on observations, comments, and lessons learned. Section VI presents conclusions and recommendations, and discusses future developments. The Act, OMB Bulletin 88-16, and the Plan Evaluation Guide are included as Appendices A, C, and D, respectively.

E.   Additional Sources of Information

To obtain NIST Publication List 91, "Computer Security Publications," and/or copies of NCSL bulletins on computer security call the National Computer Systems Laboratory (NCSL) at (301)975-2821. Publications are available through the Government Printing Office (GPO) at (202) 783-3238 and the National Technical Information Service (NTIS) at (703) 487-4780.

NIST sponsors the NCSL Computer Security Bulletin Board System with a special emphasis on information systems security issues. The bulletin board contains various types of awareness and reference materials, including bibliographies, security-related seminar and conference lists, and computer security products information. For information, please contact Marianne Swanson at (301) 975-3293.

NSA sponsors the National Computer Security Center (NCSC) Bulletin Board on DOCKMASTER which has over 3000 subscribers and serves as a focal point for interacting and exchanging computer security-related ideas amongst its users. For information, please call, in Maryland, (301) 850-4446; outside Maryland, (800) 336-3625.

NIST, in conjunction with NSA, operates a Risk Management Laboratory, at its Gaithersburg, MD facility, that investigates tools and techniques for risk management. Please address questions regarding the laboratory to Irene Gilbert of NIST at (301)975-3360.

See Appendix I, References, for other sources of information on computer security.

Questions regarding this report should be addressed to Dennis Gilbert of NIST at (301)975-3872. Questions regarding the NIST Agency Assistance Program, should be addressed to Jon Arneson of NIST at (301)975-3870.

II. DESCRIPTION OF THE CSPP REVIEW PROCESS

A.   The Joint NIST/NSA Review Team

The joint NIST/NSA Review Project convened in January 1989, one year after the enactment of Public Law 100-235. The reviewers, tasked with the responsibility of examining the plans, consisted of up to ten NIST members and twenty-two NSA members, including one NIST and one NSA project leader. In addition to providing meaningful comment on the plans, reviewers' responsibilities included safeguarding agency-specific information gained from the plan review. A commitment to confidentiality was accepted by all members to ensure that specific sensitive information within the plans would not be released by any review team member.

The joint review team was subdivided into five teams: one team to provide preliminary analysis, screening, and data recording; and four plan analysis teams to provide advice and comments on the individual plans. Each team consisted of both NIST and NSA team members and varied in size from three to six people, including a NIST or NSA senior staff member who served as team leader. Two contractor-support personnel were also assigned to the project for database work.

B.   The CSPP Evaluation Guide

The review teams based the plan review on the Plan Evaluation Guide which provided basic instructions on collecting preliminary data, and the roles and responsibilities of each member on the team. More importantly, the Plan Evaluation Guide elaborated on the requirements of OMB Bulletin 88-16, including those areas which were optional, and included an interpretation of what each section should contain. Although the guide provided the structure for the review process, it allowed the analysis teams flexibility in implementing the guide's instructions. See Appendix D for a copy of the Plan Evaluation Guide.

C.   The Civilian Agency CSPP Review Process

1.   The Review Process

An agency's submission contained one or more computer security plans (CSPPs). The review of an agency's submission followed a four-step process: 1) preliminary analysis; 2) agency program overview analysis; 3) plan analysis and comment; and 4) preparation of an agency summary. Each review team processed all of a particular agency's plans, thus providing a measure of continuity

in the review process. Because of the confidentiality issue, all plans were returned to the originating agencies along with the advice and comments and agency summaries. The review team retained only the needs and additional comments sections for work discussed in a later section.

a. Preliminary Analysis

As each agency submission was received, the preliminary review team logged each plan into a database, assigning a unique identification number, the agency name, the agency's acronym, the responsible organizational subcomponent, the operating organization, and the system's name and title. A preliminary review determined if the plan contained adequate information for a full review. The preliminary review checked for the following, as outlined in the Plan Evaluation Guide:

   o   a system description that identifies at least "generic" types of information processed (e.g., payroll, personnel, administrative) and at least "generic" types of processing to be accomplished (e.g.; financial management, decision support).

   o   a description of the reasons the system has been identified as sensitive, and an indication that at least one of the indicated sensitivity requirements (confidentiality, integrity, and availability) is a primary or secondary concern (i.e., that all three were not reported or reported as minimal).

   o   an indication that at least some of the categories of protection measures covered in OMB Bulletin 88-16 are "in place" or "planned."

Plans not containing the above were returned to the project managers who referred them to OMB for decision on whether to return them to the originating agency. Agencies that received plans returned for insufficient information were given the option of rewriting and resubmitting the deficient plans for analysis.

b. Agency Program Overview Analysis

OMB Bulletin 88-16 gave agencies the option of submitting an agency-level overview. These overviews were expected to contain information about agencywide policies, procedures, and standards, and any agency-level concerns or needs. If submitted, the review teams reviewed the agency's security plans in light of the information provided by these overviews.

c. Plan Analysis

The security plan analysis covered four distinct areas:

o   Basic System Identification

o   Sensitivity of Information Handled

o   System Security Measures

o   Needs and Additional Comments

Within each of the above areas, the bulletin called for specific items. Many of these mapped directly to areas covered by NIST standards and guidelines, and, in some cases, individual agency policies. See OMB Bulletin 88-16 and the Plan Evaluation Guide in Appendices C and D, respectively, for additional information.

Following the plan review, the team prepared advice and comment on the plan. Areas that indicated a possible discontinuity in the security planning for each were noted. Also, specific mention was made if the plan did not address key elements, such as those controls required by OMB Circular A-130, "Management of Federal Information Resources." (Note: This policy document, which applies to all executive branch agencies, directs the management of these resources and provides a series of procedural and analytical guidelines. Appendix III of the circular, entitled "Security of Federal Automated Information Systems," "establishes a minimum level of controls to be included in Federal automated information systems security programs," assigns security responsibility within agencies, and describes the relationship with the policies in OMB Circular A-123, "Internal Control Systems." Appendix III also specifies controls that must be instituted on federal systems, including personnel training, contingency planning, and certifications. See Appendix B for a copy of the circular's Appendix III.)

d. Final Agency Summary

Upon completing the review of each agency's submission, the team leader prepared an agency summary as an overview of the advice and comment for all the agency's computer security plans.

2. The Data Collection Process and Building the Database

The primary goal of the data collection process was to gather all relevant data from the civilian agency CSPPs without retaining

copies of the documents. The second goal was to ensure that all plans were tracked throughout the plan review activity and returned to the submitting agency. Because of the difference between how civilian agency and DoD submission were handled (as discussed in Section D, below), a comparable data base for DoD submissions was not maintained.

A commercial software package was used to create databases for tracking the plans throughout the review process. A custom program was developed to record data for initial logging (LOG), preliminary data analysis (PRELIM), and final data analysis (FINAL). The program automatically assigned plan numbers to each plan to facilitate easy access to information gathered.

The LOG database holds identifying information from each plan, including the originating agency, the name of each system, and the sequential plan number. This database was used as a plan tracking system and formed the basis of the other databases.

Information from the preliminary plan analysis was entered into the PRELIM database, which used parts of the LOG database. The sequence number, agency name, and plan number were automatically pulled from LOG to ensure correct and complete tracking. PRELIM contained a point of contact, system category, the type of risk analysis, and a list of security measures and their status.

The FINAL database contained keywords describing the system and its users, the system environment, the sensitivity of the information, applicable laws or regulations that affect the system, and applicable guidance. This information was gathered during the plan analysis. See the Data Analysis Section for a final list of the keywords (or descriptors) and the Plan Evaluation Guide (Appendix D) for the list of categories.

D.   Department of Defense CSPP Review Process

DoD Headquarters directed all components to submit, by August 11th, copies of their certification/accreditation documentation in order to meet the requirements of the Act. The certification/-accreditation process, particularly relevant to large, centralized computer systems, is an integral element of DoD computer security planning. In many cases, this documentation permitted the review team to review plans that were actually being used. DoD plans that were received by January 8th were reviewed in the same manner as the civilian agency plans. Discussion and summary statistics for the civilian agency plans include the information derived from these "early" DoD submissions.

Because of the high volume and differences of the "later" DoD

submissions responding to the August 11th deadline, the review team followed a different review process. This process began with the elimination of the preliminary review. The logging procedure reflected only the submission number, the sequence number, the name of the submitting facility, activity or command, and the number of plans which fell into broad categories, such as personal computers, mainframes, minicomputers, and word processors/memory typewriters.

Most of the DoD plans included some combination of the following documentation: accreditation requests and/or approvals to operate, risk management reviews, facility security profiles, risk analysis checklists, system description sheets, letters of certification, equipment lists, and formal risk analyses. Very few of the DoD submissions were prepared in accordance with OMB Bulletin 88-16. In general, the plans did not include the information requested by the bulletin. Unlike civilian agency plans, the absence of a control did not necessarily mean that the control was not in place. However, one could not assume that proper controls were in place. Therefore, a paragraph similar to the following was included in the responses to indicate the team's mission and objectives in the plan review process:

> The Computer Security Act defines information sensitivity in terms of confidentiality, availability, and integrity. It requires agencies to consider the magnitude of the consequences that could result from the disclosure, alteration, or destruction of the system or data. Therefore, the review team considered these issues in the review of the CSPPs. ... Computer security planning involves the analysis of the nature of the system, its operational environment, and the sensitivity of the data. This process should result in the selection and implementation of cost effective controls and protections appropriate to the potential for loss or harm.

In addition to providing a reminder about the security awareness and training requirements of the Act, the team also noted any indications of items that could impact on the confidentiality, integrity, and availability of the information processed.

Following the team's review of the DoD plans, comments were provided on a per submission basis, rather than on a per plan basis as for the civilian agencies. In some cases, this resulted in one set of advice and comment for an entire base or installation.

III. DATA ANALYSIS

A. Introduction

The data collected during the plan review process is presented in this section in tabular and graphic form.   The data is what was reported in and extrapolated from the CSPPs. The data represents the subjective judgements of those who prepared the plans and may not be, therefore, a true representation of the federal systems reported.

B. Presentation of Data

The 63 civilian agencies that submitted 1,583 CSPPs are listed in Tables III-1 through III-4. The agencies have been grouped into the three branches of government (executive, legislative, and judicial). The executive branch has been broken down into cabinet and independent establishments. (Note: Veterans Administration, which is now the Department of Veterans Affairs, is included under independent establishments. This reflects its status at the time of CSPP submission.)

EXECUTIVE BRANCH: CABINET AND EXECUTIVE OFFICE

AGENCY	
Department of Agriculture	70
Department of Commerce	84
Department of Education	61
Department of Energy	80
Department of Health and Human Services	92
Department of Housing and Urban Development	48
Department of the Interior	155
Department of Justice	83
Department of Labor	78
Department of State	15
Department of Transportation	89
Department of the Treasury	87
Executive Office of the President	13
Federal Energy Regulatory Commission	16
Office of the U.S. Trade Representative	3

Total Number of Plans = 974

Table III-1 -   CSPPs from Cabinet and Executive Office

EXECUTIVE BRANCH: INDEPENDENT ESTABLISHMENTS AND CORPORATIONS

<u>AGENCY</u>

Agency for International Development	17
Appalachian Regional Commission	1
Architectural & Transportation Barriers Compliance Board	1
Commodity Futures Trading Commission	5
Consumer Product Safety Commission	3
Environmental Protection Agency	28
Equal Employment Opportunity Commission	5
Export-Import Bank of the United States	4
Federal Communications Commission	4
Federal Election Commission	4
Federal Emergency Management Agency	3
Federal Home Loan Bank Board	1
Federal Trade Commission	6
General Services Administration	32
International Trade Commission	5
Merit Systems Protection Board	6
National Aeronautics and Space Administration	88
National Archives and Records Administration	3
National Capitol Planning Commission	1
National Credit Union Administration	14
National Endowment for the Arts	6
National Endowment for the Humanities	6
National Labor Relations Board	5
National Mediation Board	1
National Science Foundation	8
Nuclear Regulatory Commission	47
Occupational Safety and Health Review Commission	1
Office of Personnel Management	46
Office of the Special Counsel	2
Overseas Private Investment Corporation	11
Panama Canal Commission	7
Peace Corps	4
Pension Benefit Guarantee Corporation	11
Railroad Retirement Board	9
Securities and Exchange Commission	12
Selective Service System	9
Small Business Administration	14
Tennessee Valley Authority	1
U.S. Information Agency	8
Veterans Administration	71
Total Number of Plans = 510	

Table III-2   -   CSPPs from Independent Establishments

LEGISLATIVE BRANCH

AGENCY

Congressional Budget Office	3
General Accounting Office	11
Government Printing Office	1
Library of Congress	70
Office of Technology Assessment	3

Total Number of Plans = 88

Table III-3 - CSPPs from Legislative Branch Agencies

JUDICIAL BRANCH

AGENCY

Administrative Office of the U.S. Courts	8
Federal Judicial Center	2
Supreme Court of the United States	1

Total Number of Plans = 11

Table III-4 - CSPPs from Judicial Branch Agencies

Figure III-1 shows the distribution of civilian agency CSPPs by branch of government.
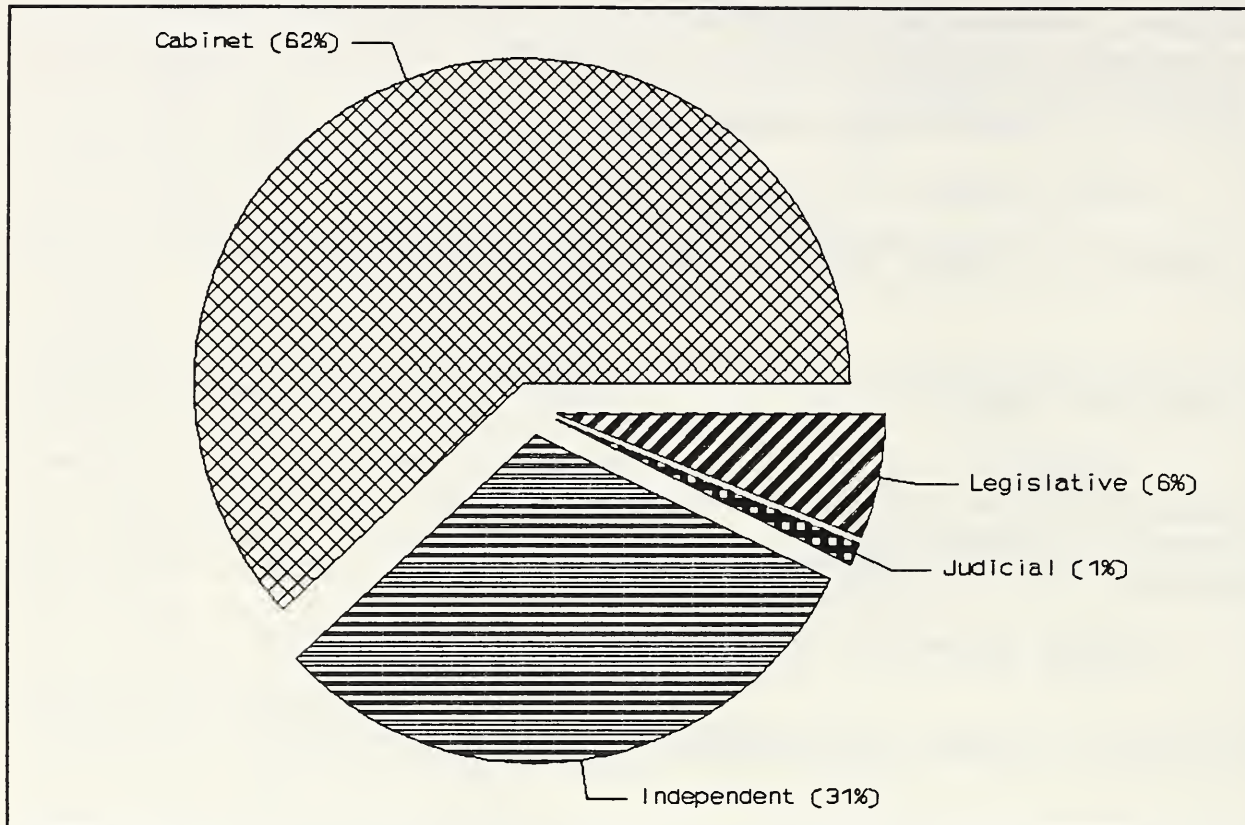
Figure III-1 — Civilian Agency CSPP Distribution by Branch of Government

C. Civilian Agency Plan Profile

This section presents the civilian agency data as well as the data for the 55 plans that were submitted by January 8, 1989 by DoD. The data is presented in the same format used in OMB Bulletin 88-16: Basic System Identification, Sensitivity of Information Handled, and System Security Measures. Needs and Additional Comments, a fourth area covered in the Bulletin, is addressed in Section IV.R, among lessons learned from the review process.

1. Basic System Identification

The system identification categories addressed in this section are listed below along with the allowable entries. Further information is available in Appendix C, OMB Bulletin 88-16.

System Category:	Major Application System (MAS) or General ADP Support System (GADPS)
Operational Status:	Operational, under development, or both
General Description:	A brief (one or two) paragraph of the function and purpose of the system.
System Environment:	Although this section addressed all aspects of the environment, only the data on hardware was clear enough to be presented.

Further breakdowns by system category and operational status are presented in Section III.D.

Figure III-2 shows that approximately two-thirds of the CSPPs are for Major Application Systems (MAS). The remaining one-third are categorized as General ADP Support Systems (GADPS).

General ADP Support Systems (35%)

Major Application Systems (65%)
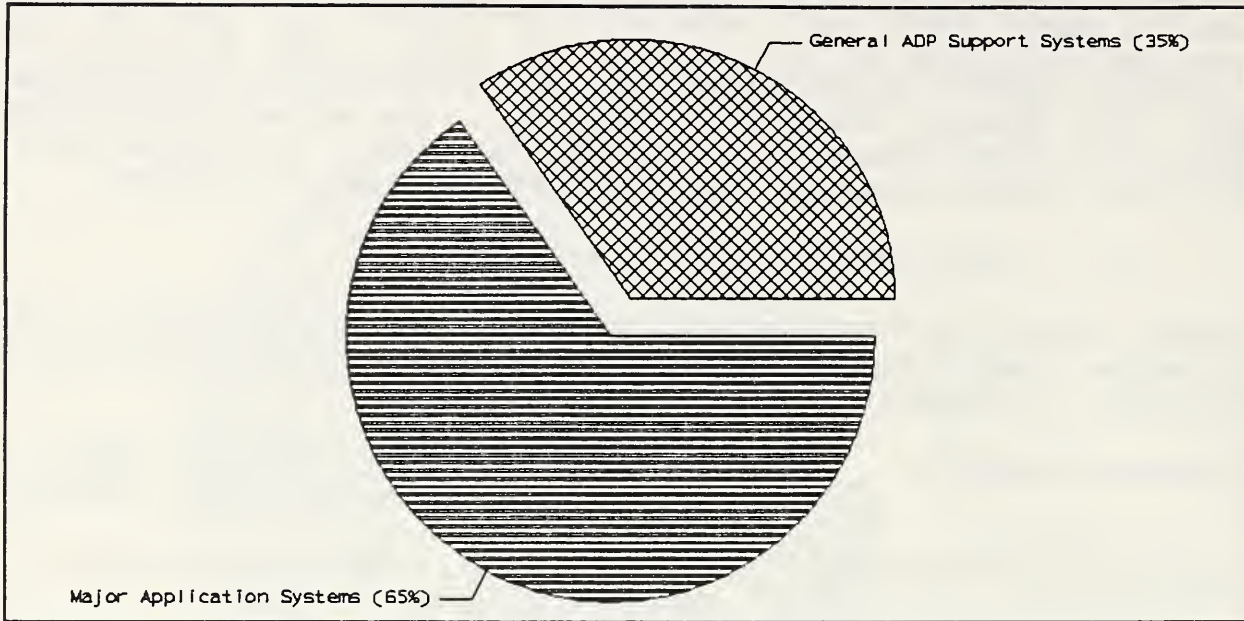
Figure III-2   -   Distribution of CSPPs by System Category

Figure III-3 shows that most of the CSPPs reported on operational systems.

Operational (89%)

Op & Und Devel (3%)

Under Devel (8%)
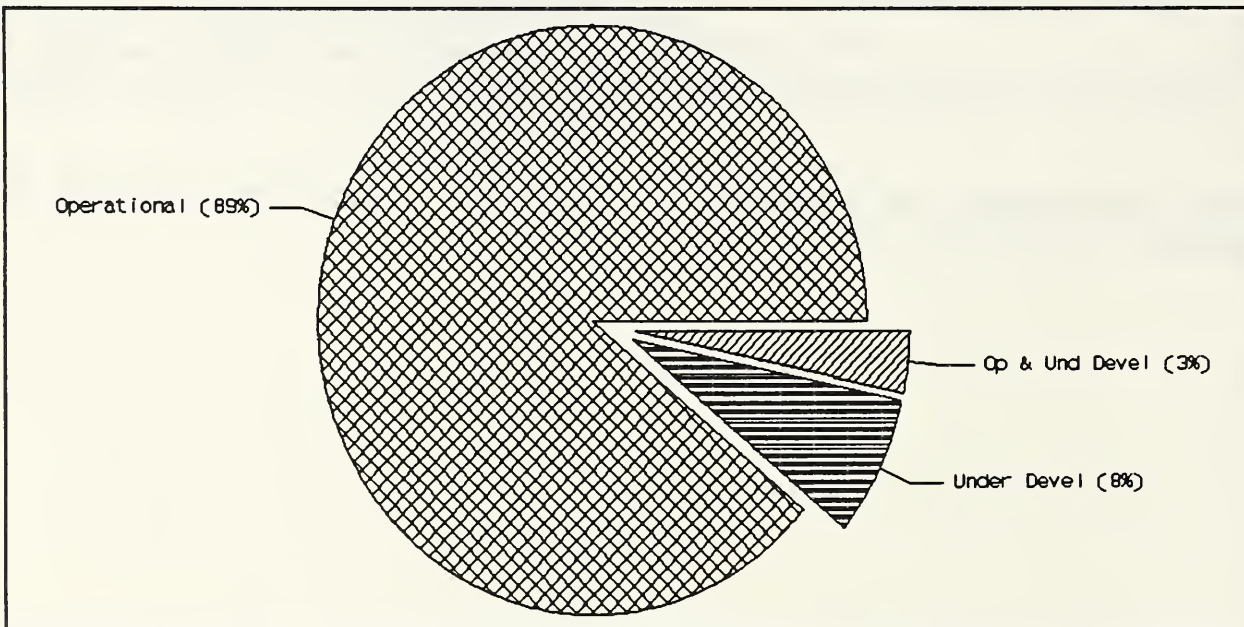
Figure III-3   -   Distribution of CSPPs by Operational Status

III-6

The entries for General Description and System Environment were based on key words. Key wording was based on the content of the plan. However, the reviewer was often required to extrapolate based on knowledge and experience. Multiple entries were allowed for each field. For example, more than one type of hardware can be in use in a system. Therefore, the percentages can total more than 100 percent. Similar categories of key words were combined to present clearer trends to the data.

Table III-5 shows that financial, managerial, and administrative information are most often identified in the CSPPs.

GENERAL DESCRIPTION/PURPOSE	PERCENTAGE
Financial	29
Management Information	28
Administration	16
Personnel	11
Office Automation	10
Recordkeeping/Reporting	9
Engineering & Science	8
ADP/AIS Facility	8
Law Enforcement/Judicial	6
Health and Safety	6
Transportation/Travel	5
Miscellaneous Support	5
Science Applications	5
Audit	5
Telecommunication/Remote Process	5
Procurement	3
Miscellaneous	3
Insurance	2
Earth Science	2
Not Reported	2
	---
	168 *

Table III-5 - Distribution by General Description/Purpose

* This table contains non-mutually exclusive fields causing the total to exceed 100%. An amount over 100% represents the existence of plans which reported more than one item for this category.

Table III-6 shows generic types of computer hardware reported by the CSPPs.

SYSTEM ENVIRONMENT/HARDWARE	PERCENTAGE
Mainframe	47
Networked	36
Microcomputer-based	29
Minicomputer	20
Database Management System	6
	---
	138 *

Table III-6 - Distribution by Environment/Hardware

* This table contains non-mutually exclusive fields causing the total to exceed 100%. An amount over 100% represents the existence of plans which reported more than one item for this category.

2.   Sensitivity of Information Handled

The information sensitivity addressed in this section is broken down into two parts:

Part 1

Type of Information:	Generic types of sensitive information handled by the system.
Impacts:	The potential damage which might occur through error, unauthorized disclosure, modification, or unavailability

Part 2

System Protection Requirements:	The need for confidentiality, integrity, and availability.

Like general description and system environment, entries for sensitivity of information were based on key words derived from the plan contents. Here, too, the reviewer was often required to extrapolate based on knowledge and experience. Multiple entries were allowed for each field. Therefore, the percentages can total more than 100 percent. Similar categories of key words were combined to present clearer trends to the data.

The generic types of information are shown in Table III-7. This table is based on plans for which the review team was able to extract type of information data.

INFORMATION SENSITIVITY TYPE OF INFORMATION	PERCENTAGE
Privacy Act Data	44
Mission Critical	33
Financial/Budget/Government Assets	23
Proprietary	10
Management Private	9
Sensitive Until Released	7
Audit/Investigative	7
Technologically Sensitive	5
Sensitive/Restrictive	2
Non-Sensitive	2
Nuclear	2
	----
	144 *

Table III-7 — Distribution by Type of Information
* This table contains non-mutually exclusive fields causing the total to exceed 100%. An amount over 100% represents the existence of plans which reported more than one item for this category.

Table III-8 shows the loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. This table is based on plans for which the review team was able to extract impact data.

INFORMATION SENSITIVITY - IMPACT	PERCENTAGE
Impairment of Agency in Performance of Mission	34
Inaccurate Information/Reporting	23
Lawsuit	22
Inconvenience to Gov't in Performance of Mission	13
Loss of Gov't Assets	12
Embarrassment to Agency/Loss of Confidence	10
Personal/Corporate Gain	10
Life Threatening/Death	3
Prohibited Technology Transfer	1
	---
	128 *

Table III-8 — Distribution by Impact
* This table contains non-mutually exclusive fields causing the total to exceed 100%. An amount over 100% represents the existence of plans which reported more than one item for this category.

Figure III-4 and Table III-9 show overall federal management
decisions about the relative importance of protection requirements
for each of the three categories of sensitivity (confidentiality,
integrity, and availability). See IV.S (What was Reported VS. What
was Communicated) for more information.
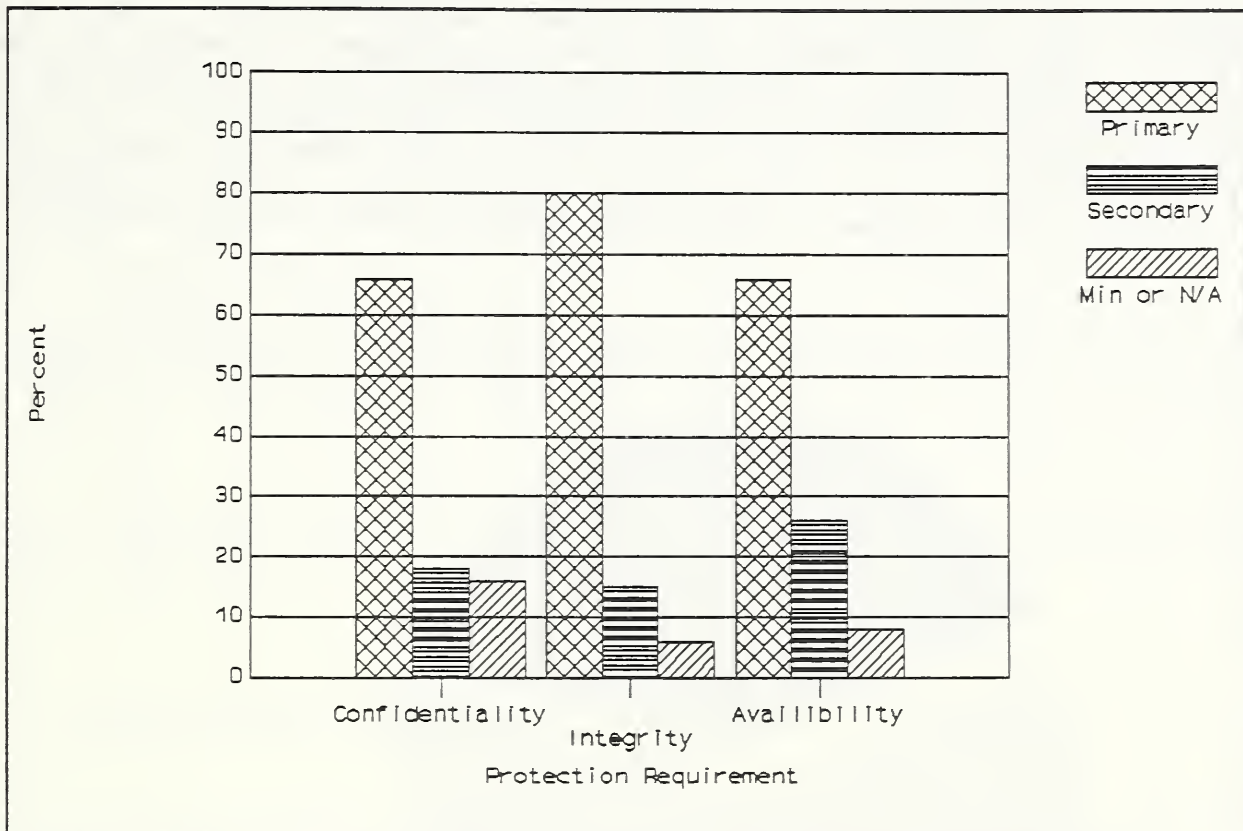
Figure III-4 - Distribution by Protection Requirements

PROTECTION REQUIREMENTS	PRIMARY	SECONDARY	MINIMAL OR N/A
CONFIDENTIALITY	66%	18%	16%
INTEGRITY	80%	15%	5%
AVAILABILITY	66%	26%	8%

Table III-9 - Distribution by Protection Requirements

3.   System Security Measures

This section of OMB Bulletin 88-16 addressed two questions: the method of risk assessment used and the security measure status.

The risk assessment field was used to report on the nature of performed risk assessments. Respondents could indicate whether a "formal," "other," or "formal and other" assessment methodology was used. The distribution is shown in Figure III-5. This field, however, did not address whether a risk assessment had actually been performed. In fact, of the plans that reported some risk assessment methodology, 19% did not report that a risk assessment was "in place or planned" under the management controls section.
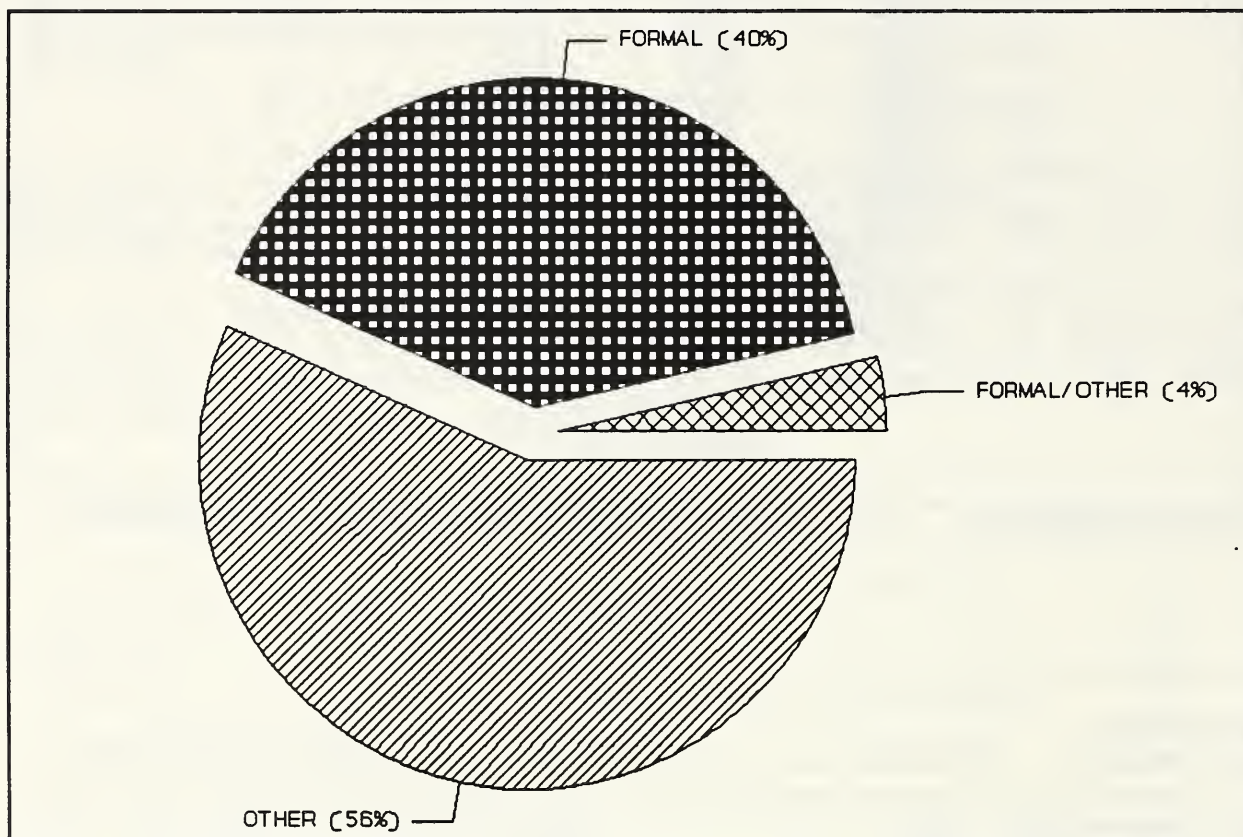
Figure III-5   -   Percentage of CSPPs Reporting Type of Risk Assessments

The status of the reported security measures are presented in Tables III-10 and III-11 and Figures III-6 through III-38 following the tables. These tables and figures divide the CSPPs into General ADP Support Systems (GADPS) (Table III-10 and Figures III-6 through III-22) and Major Application Systems (MAS) (Table III-11 and Figures III-23 through III-38).

As shown in Table III-10 and Table III-11 and Figures III-6 through III-38, the vast majority of the controls are reported either in place or in place and planned. The notable exception is certification/accreditation, which is reported less than 60 percent in place or in place and planned. Also, integrity and confidentiality controls for General ADP Support System (GADPS) are reported only approximately 80% in place or planned. OMB Bulletin 88-16 defined these controls narrowly as encryption, message authentication, and other technical mechanisms. On the other hand, integrity controls for Major Application Systems (MAS), which were 94% in place and planned, include a broad array of data validation mechanisms, such as edit checks and processing integrity checks.

Note: Since many of the plans contained blanks in the control lists, the total numbers of CSPPs reported for the various controls are not the same.

System Security Measures
GENERAL ADP SUPPORT SYSTEMS
(GADPS)

CONTROLS	TOTAL	IN PLACE	IN PLACE &PLANNED	PLANNED	N/A
Management Controls					
Assignment of Security Responsibility	520	90%	7%	2%	1%
Personnel Select/Screening	494	78%	10%	3%	9%
Risk Analysis/Assessment	468	65%	15%	16%	4%
Development Controls					
Certification/Accreditation	462	42%	8%	19%	31%
Security/Acquisition Specs	469	71%	6%	4%	19%
Operational Controls					
Audit & Variance Detection	474	68%	7%	9%	16%
Documentation	495	81%	9%	6%	4%
Physical/Environ Protect	487	86%	9%	4%	1%
Production, I/O Controls	477	78%	5%	5%	12%
Emergency,Backup,Contingency	508	64%	19%	14%	3%
System Software/Maintenance	485	82%	7%	5%	6%
Security Awareness/Training	520	60%	27%	11%	2%
Technical Controls					
Authorization/Access Control	517	83%	5%	6%	6%
Audit Trail Mechanisms	492	74%	7%	6%	13%
Confidentiality Controls	475	67%	5%	8%	20%
Integrity Controls	460	68%	5%	6%	21%
User ID & Authentication	515	79%	8%	5%	8%

Table III-10 - Distribution by Security Control Measures and Status for General ADP Support Systems
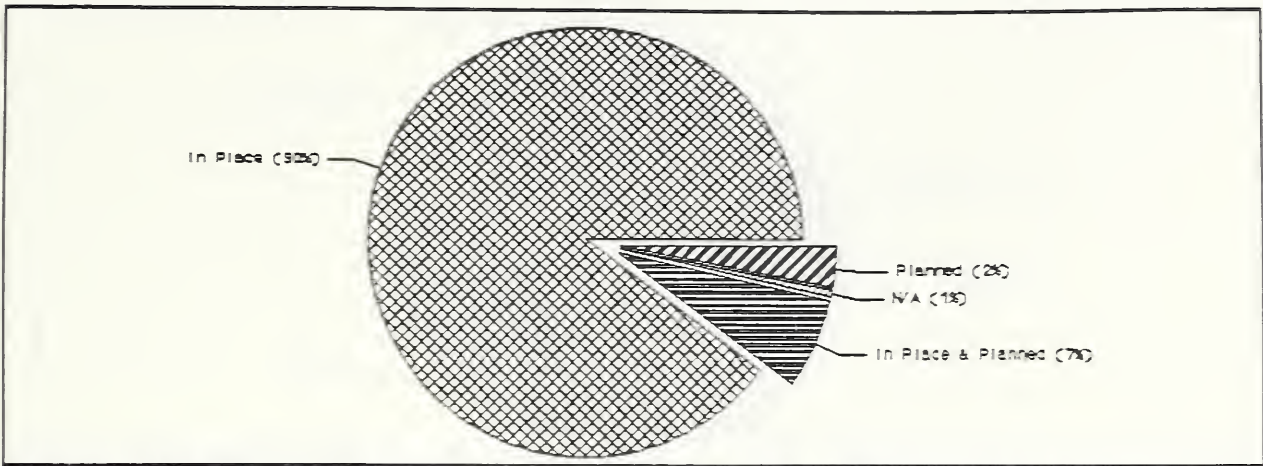
Figure III-6 - Assign. of Security Responsibility-GADPS
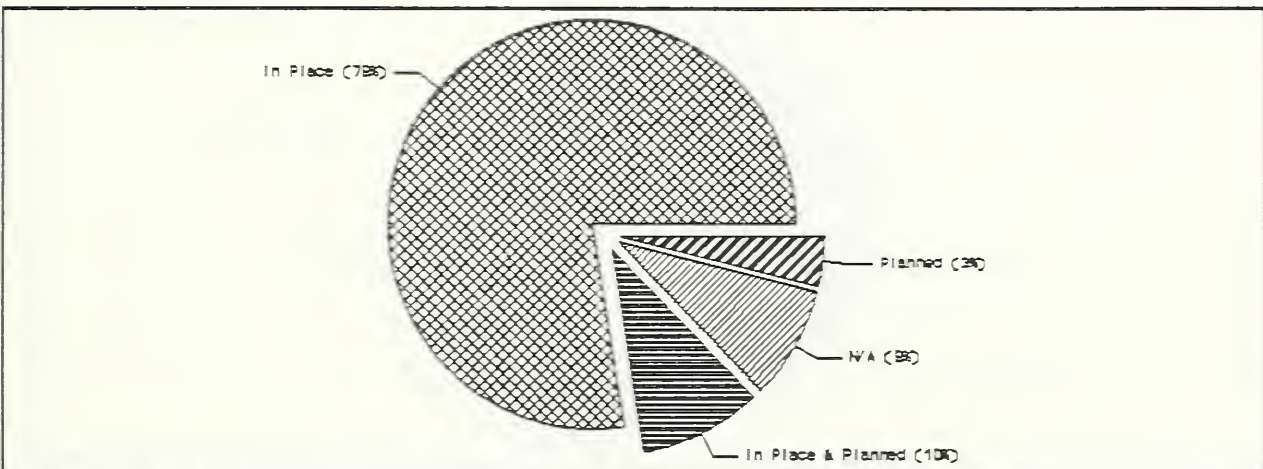
Figure III-7 - Personnel Selection and Screening-GADPS
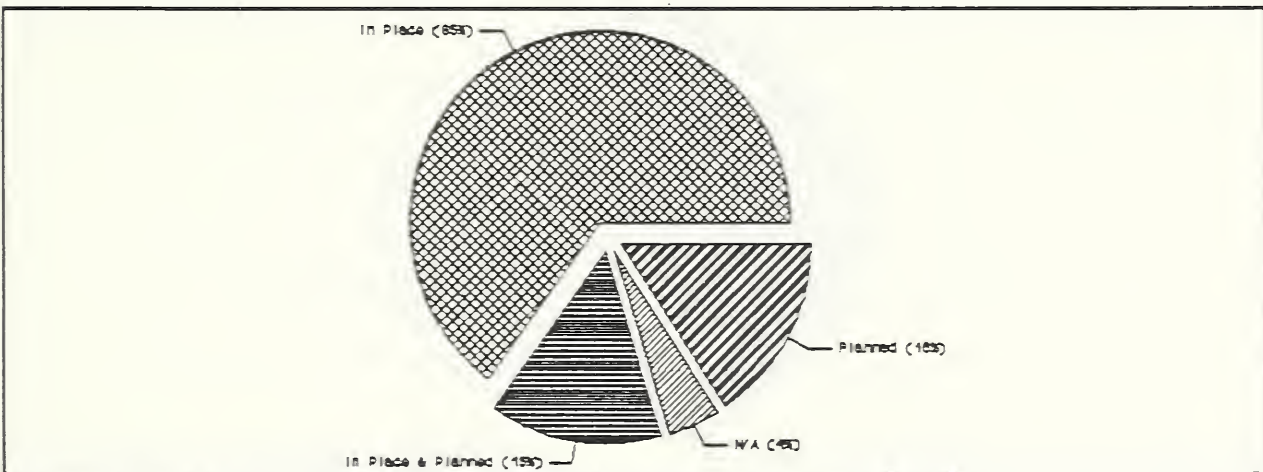
Figure III-8 - Risk Analysis/Assessment-GADPS

III-15
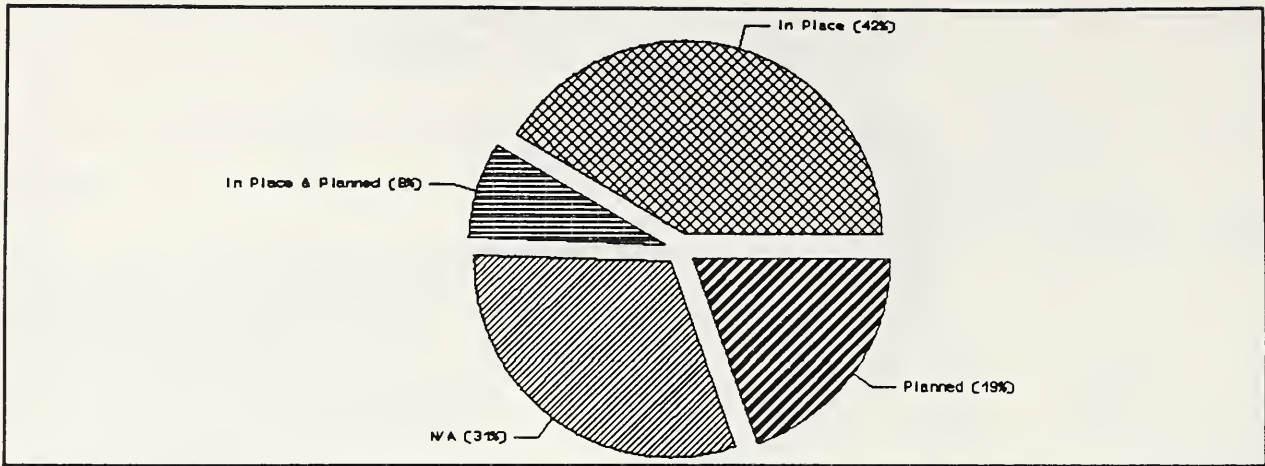
Figure III-9 - Certification and Accreditation-GADPS
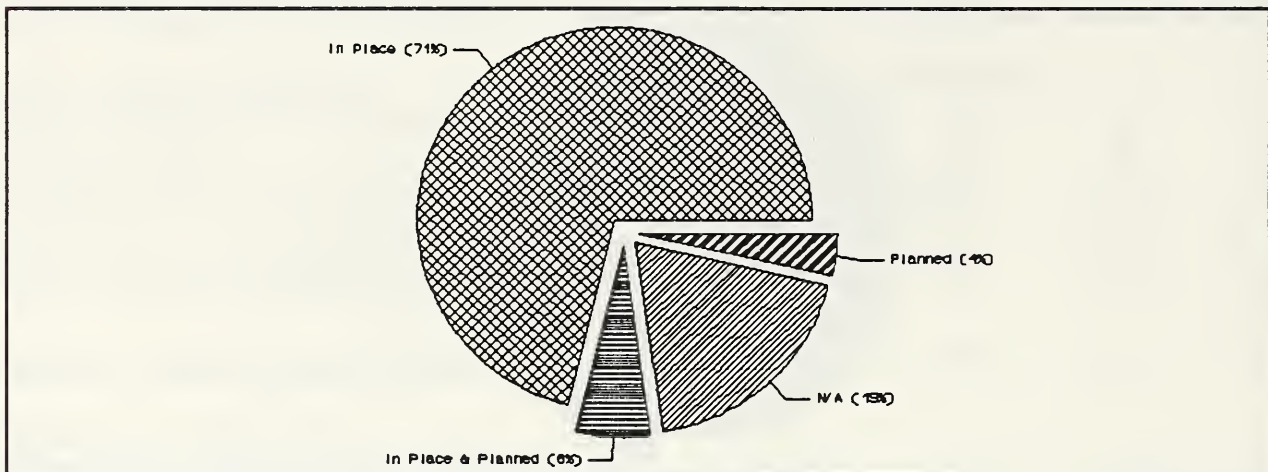
Figure III-10 - Security and Acquisition Specs-GADPS
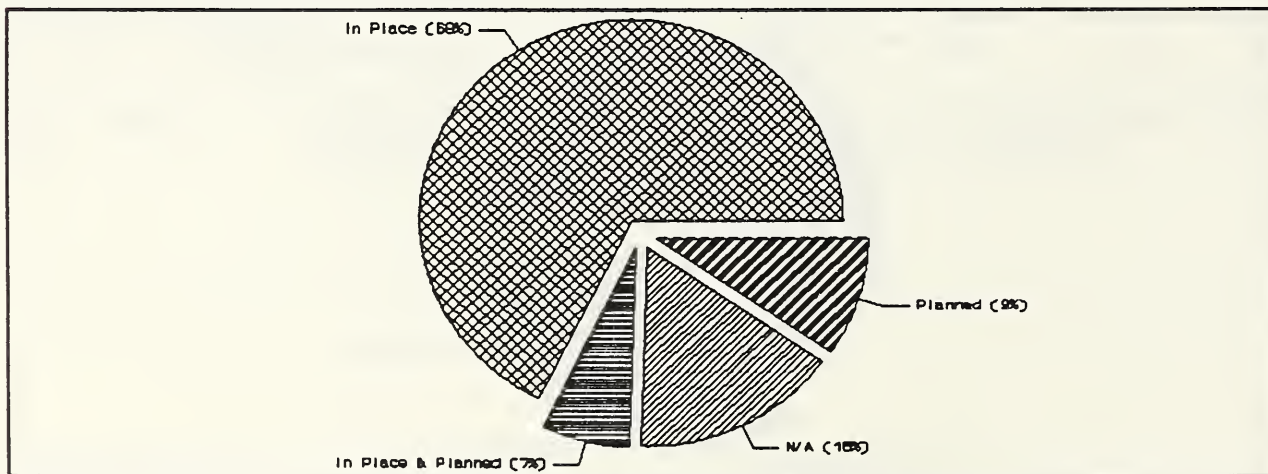
Figure III-11 - Audit/Variance Detection-GADPS
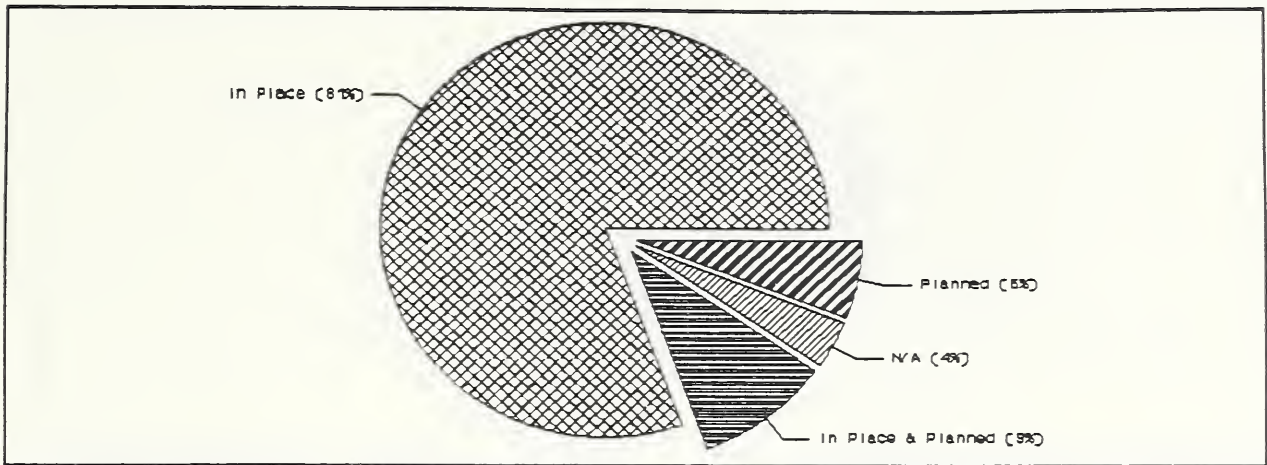
Figure III-12 - Documentation-GADPS
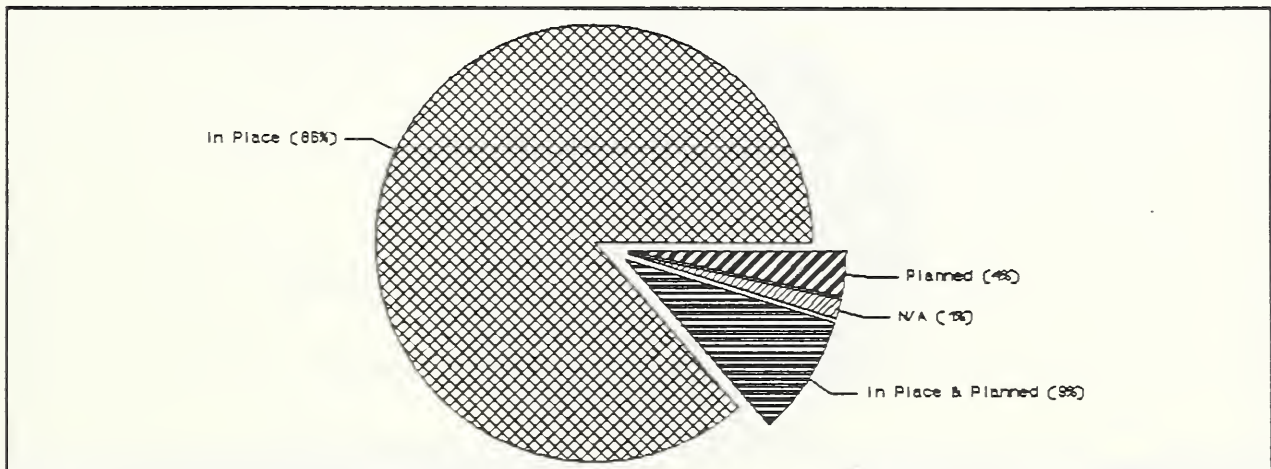
Figure III-13 - Physical/Environmental Protection-GADPS
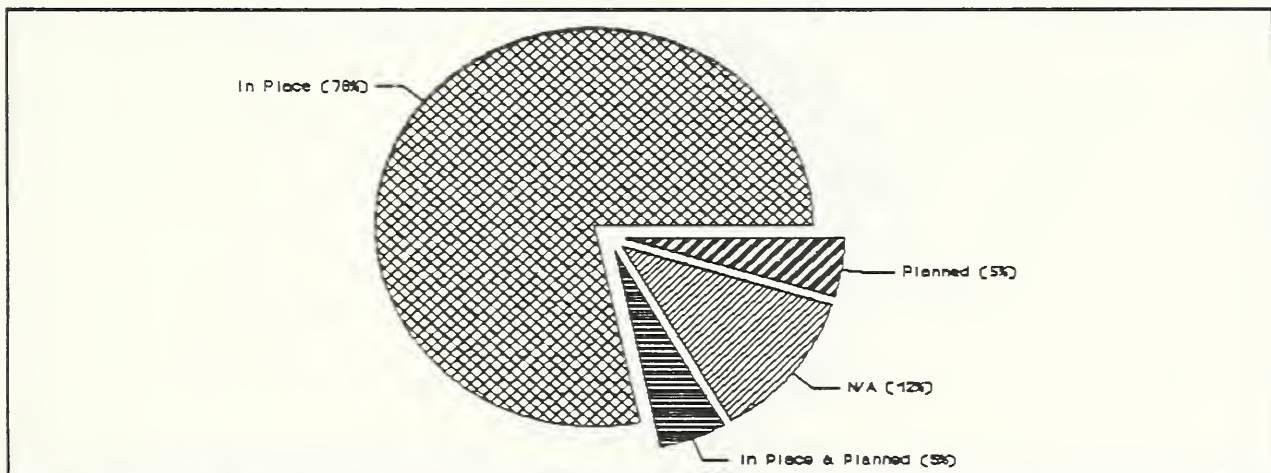
Figure III-14 - Production, I/O Controls-GADPS
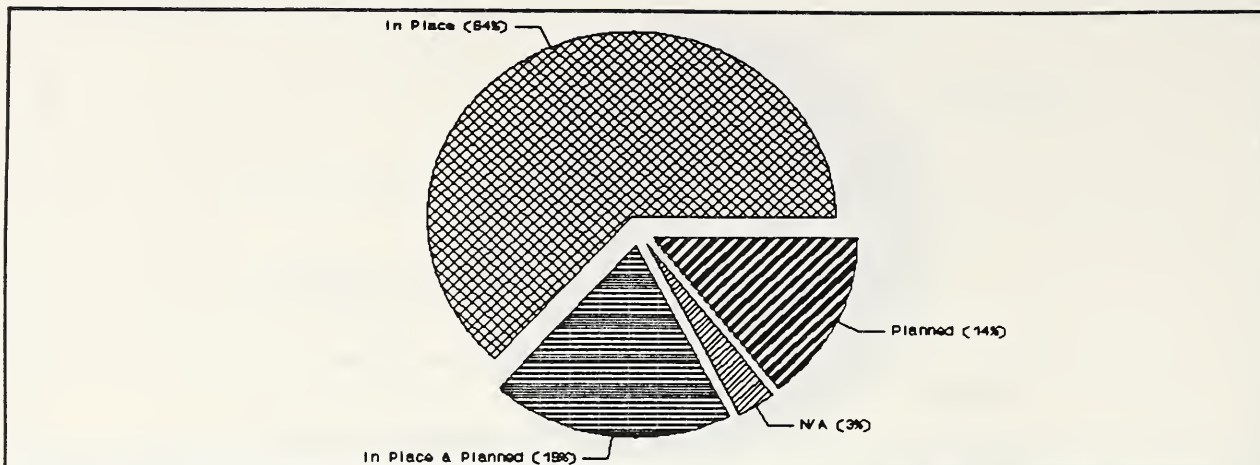
III-17

Figure III-15 - Emergency, Backup, and Cont. Planning-GADPS
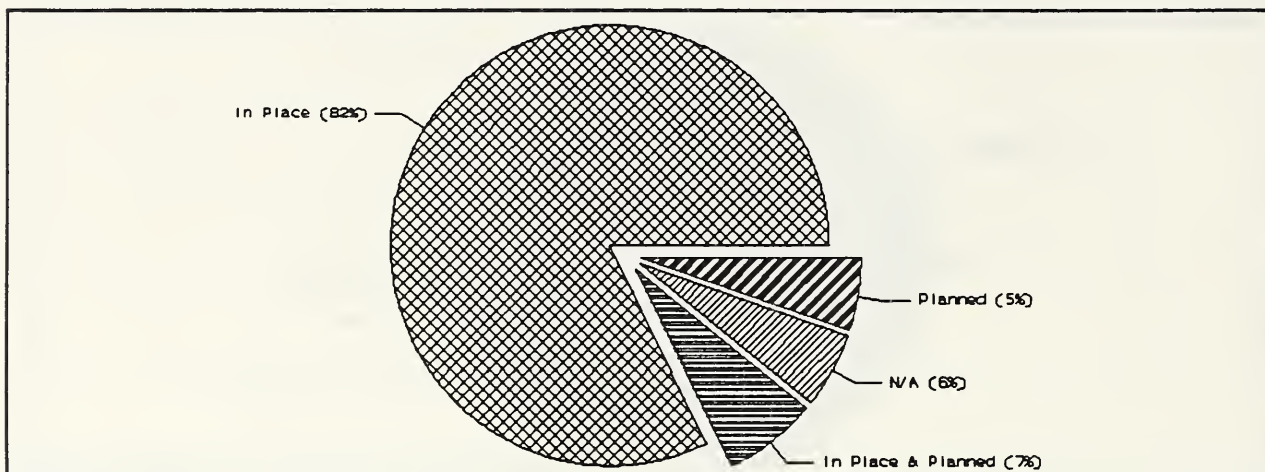
Figure III-16 - System Software and Maintenance-GADPS
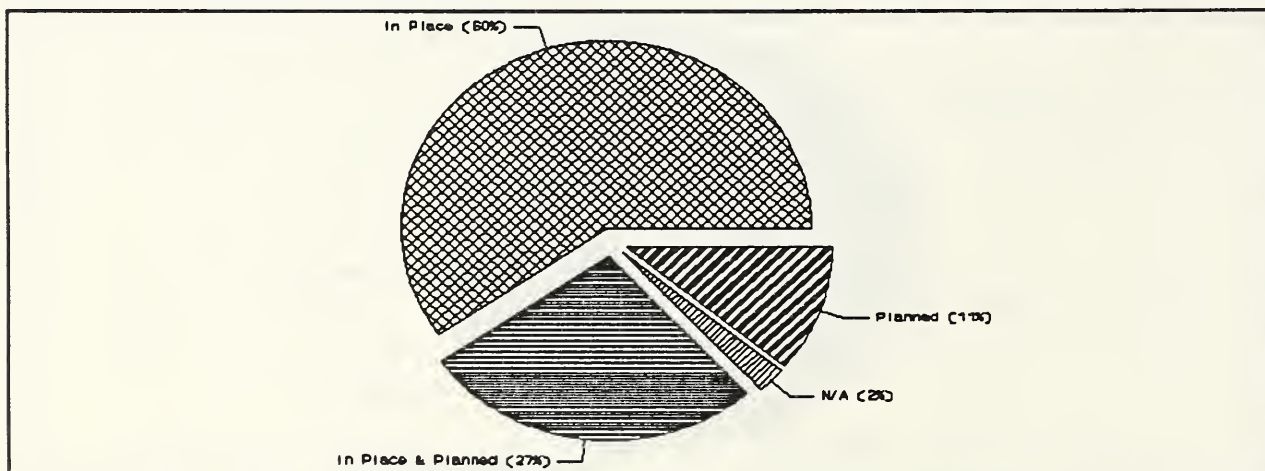
Figure III-17 - Security Awareness and Training-GADPS
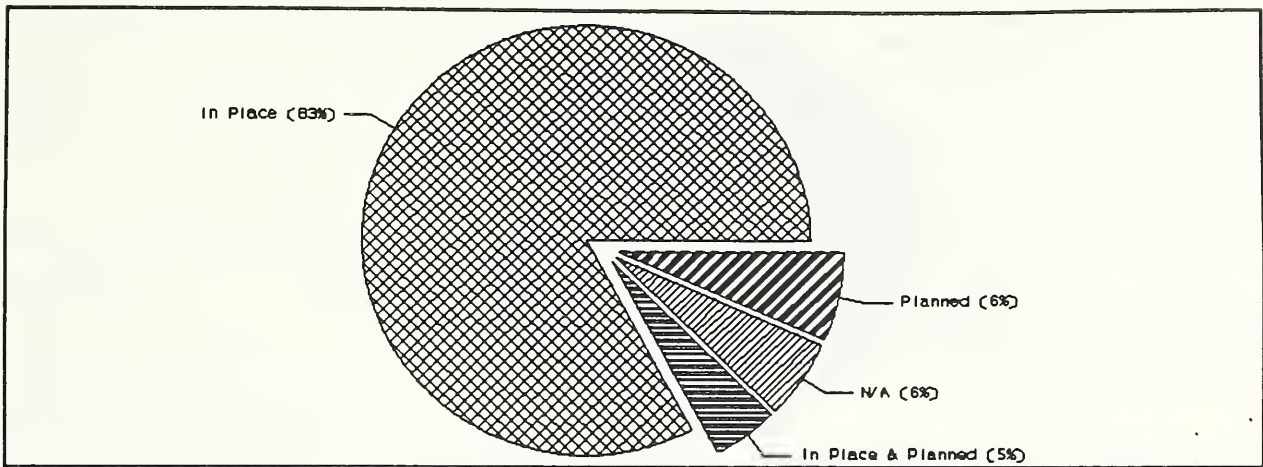
Figure III-18 – Authorization and Access Controls-GADPS
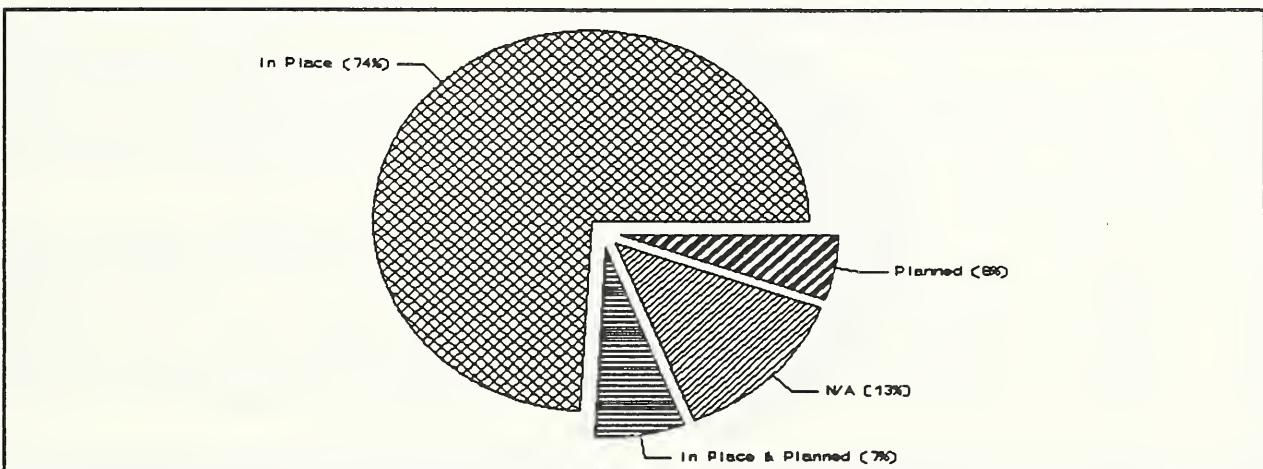
Figure III-19 – Audit Trail Mechanisms-GADPS
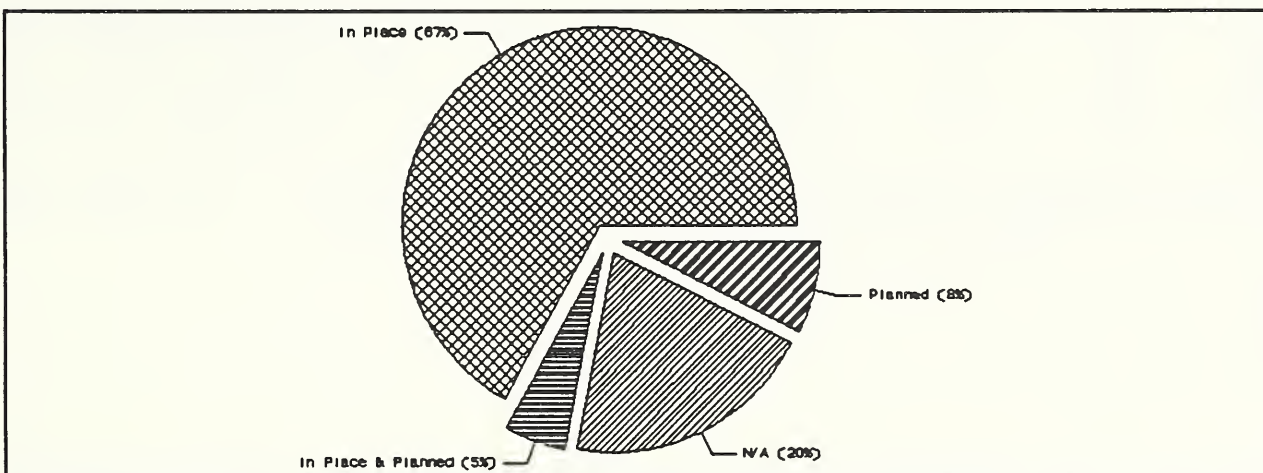
Figure III-20 – Confidentiality Controls-GADPS
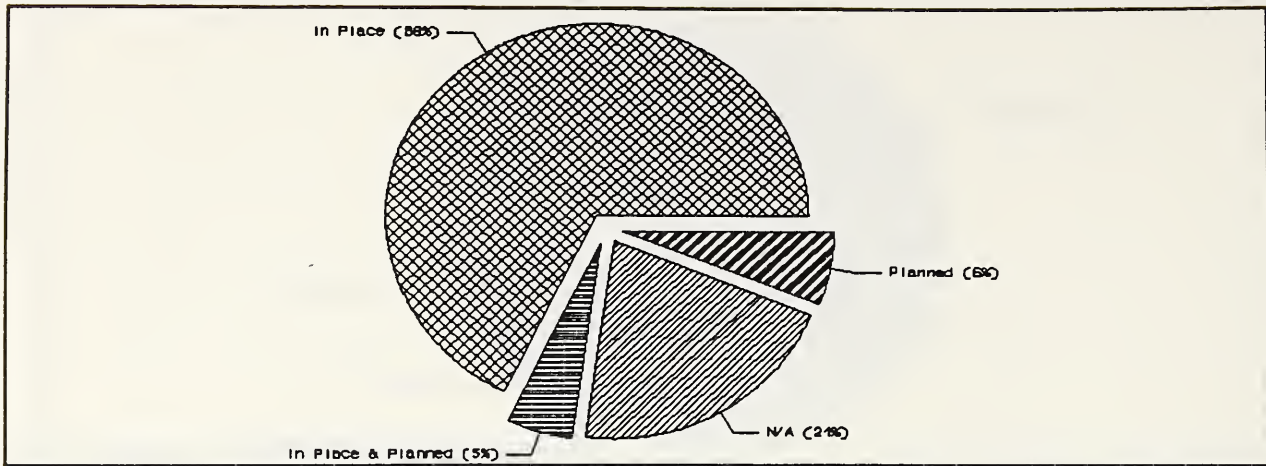
Figure III-21 - Integrity Controls-GADPS
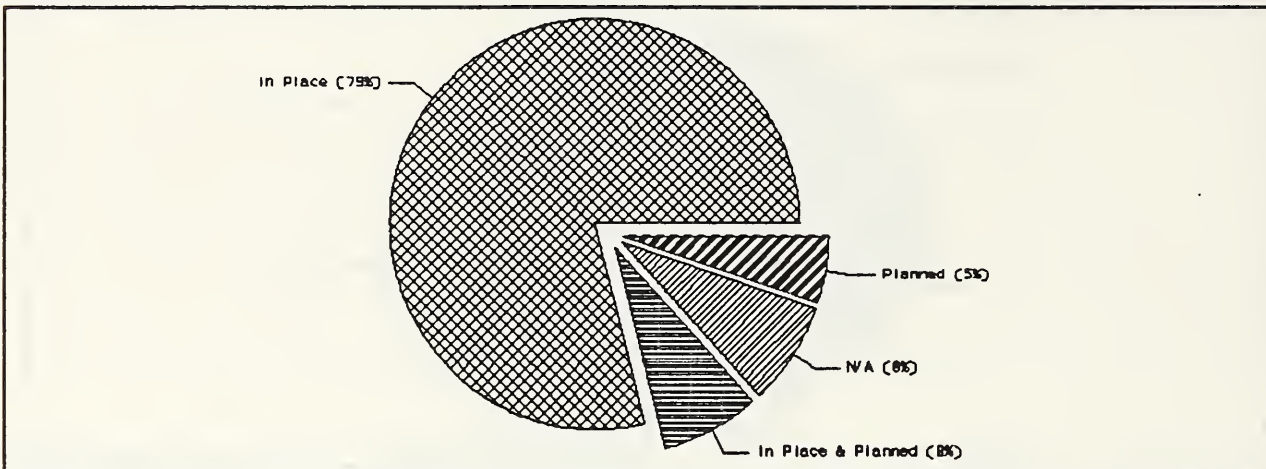
Figure III-22 - User Identification/Authorizations-GADPS

System Security Measures
MAJOR APPLICATION SYSTEMS
(MAS)

CONTROLS	TOTAL	IN PLACE	IN PLACE &PLANNED	PLANNED	N/A
Management Controls					
Assignment of Security Responsibility	986	91%	4%	5%	0%
Personnel Select/Screening	958	76%	10%	4%	10%
Risk Analysis/Assessment	953	71%	10%	16%	3%
Development Controls					
Design Review/Testing	935	65%	8%	7%	20%
Certification/Accreditation	931	47%	7%	18%	28%
Security/Acquisition Specs	932	65%	9%	7%	19%
Operational Controls					
Audit & Variance Detection	934	72%	6%	10%	12%
Documentation	959	81%	9%	9%	1%
Production, I/O Controls	953	82%	6%	7%	5%
Emergency,Backup,Contingency	976	68%	10%	18%	4%
System Software/Maintenance	951	84%	6%	6%	4%
Security Awareness/Training	970	57%	24%	17%	2%
Technical Controls					
Authorization/Access Control	977	85%	6%	6%	3%
Audit Trail Mechanisms	947	71%	7%	8%	14%
Integrity Controls	953	81%	7%	6%	6%
User ID & Authentication	986	84%	6%	6%	4%

Table III-11 – Distribution by Security Control Measures and Status for Major Application Systems
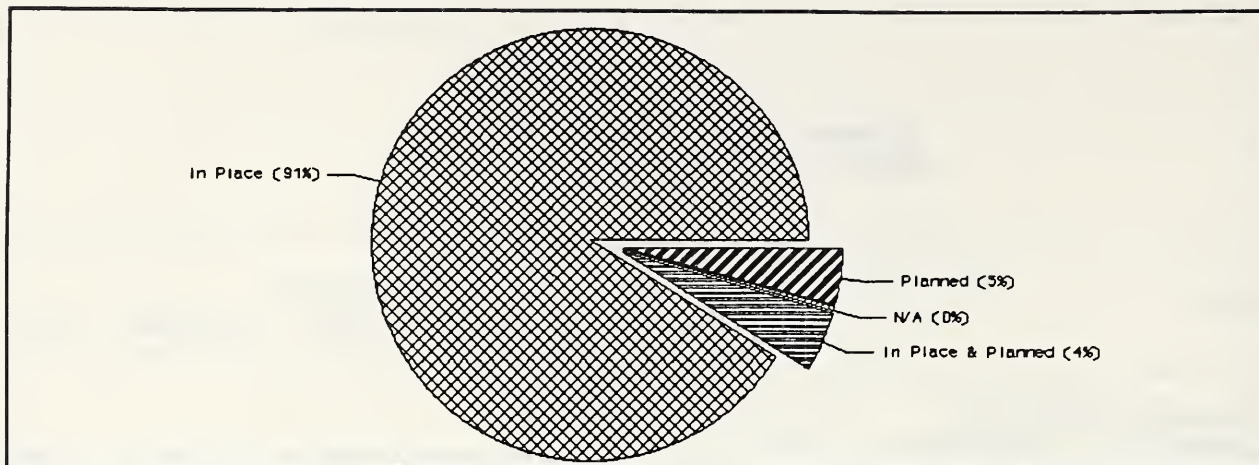
Figure III-23 -   Assignment of Security Responsibility-MAS
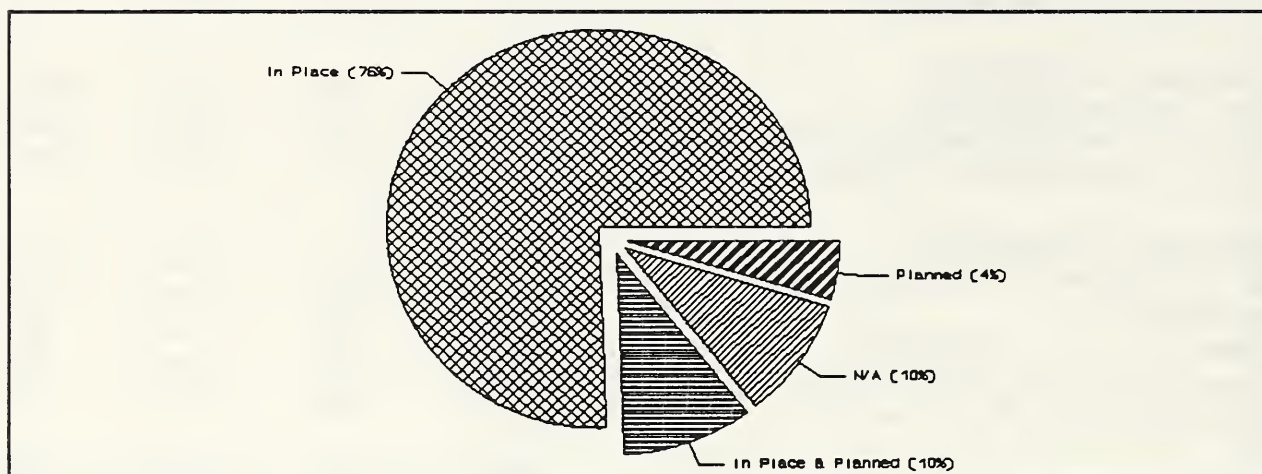
Figure III-24 -   Personnel Selection and Screening-MAS
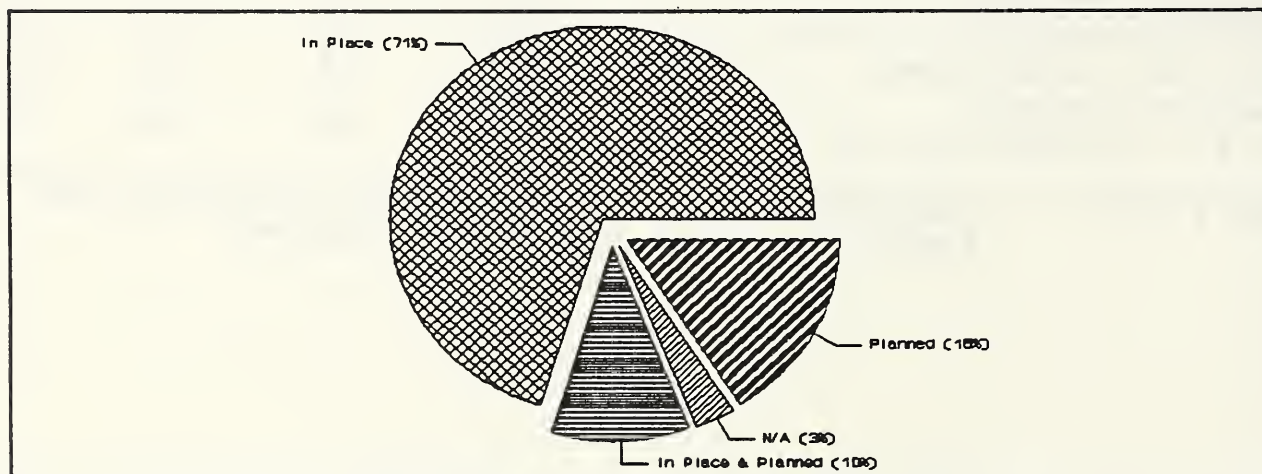
Figure III-25 -   Risk Analysis/Assessment-MAS
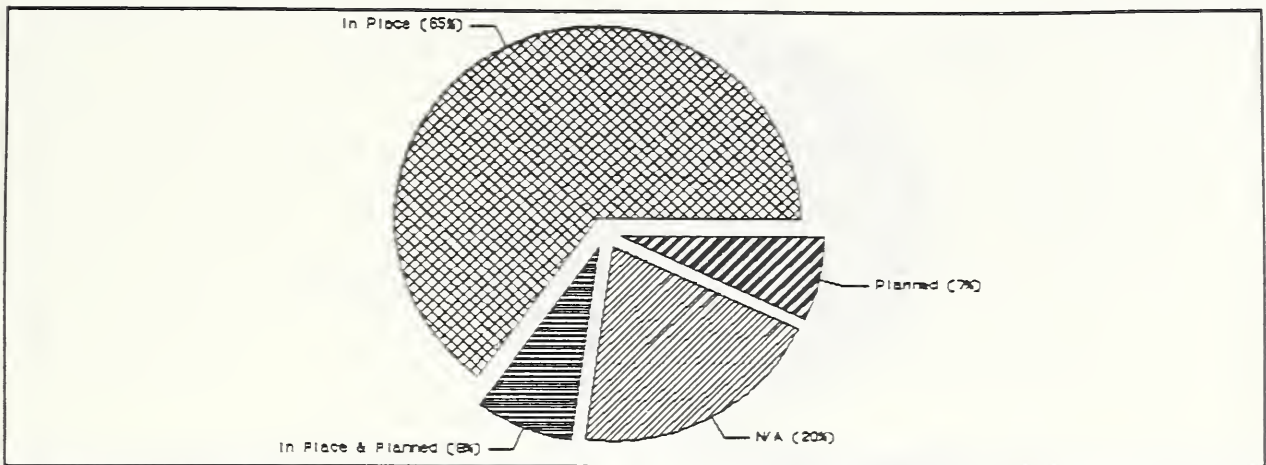
Figure III-26 - Design Review and Testing-MAS
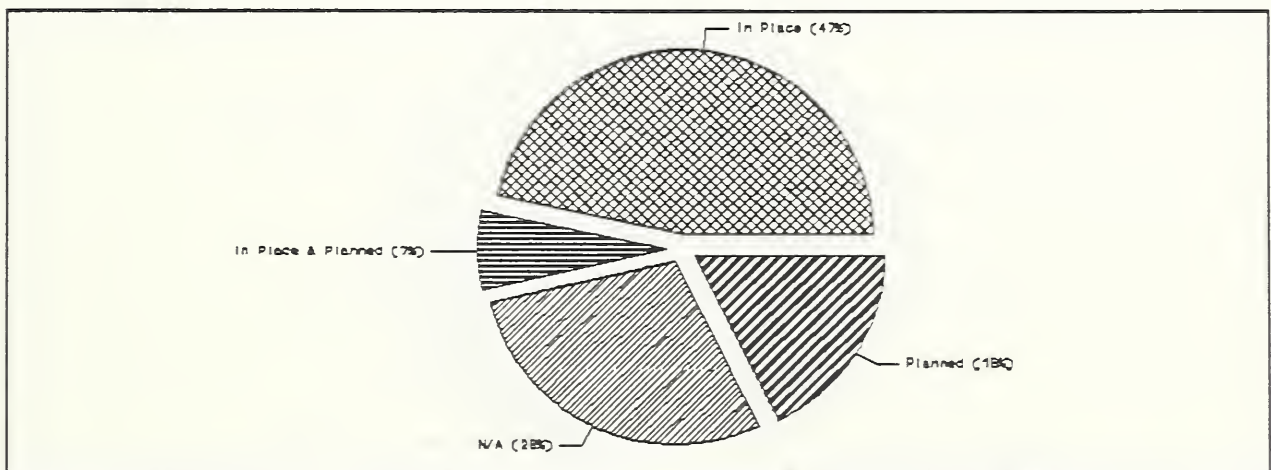
Figure III-27 - Certification and Accreditation-MAS
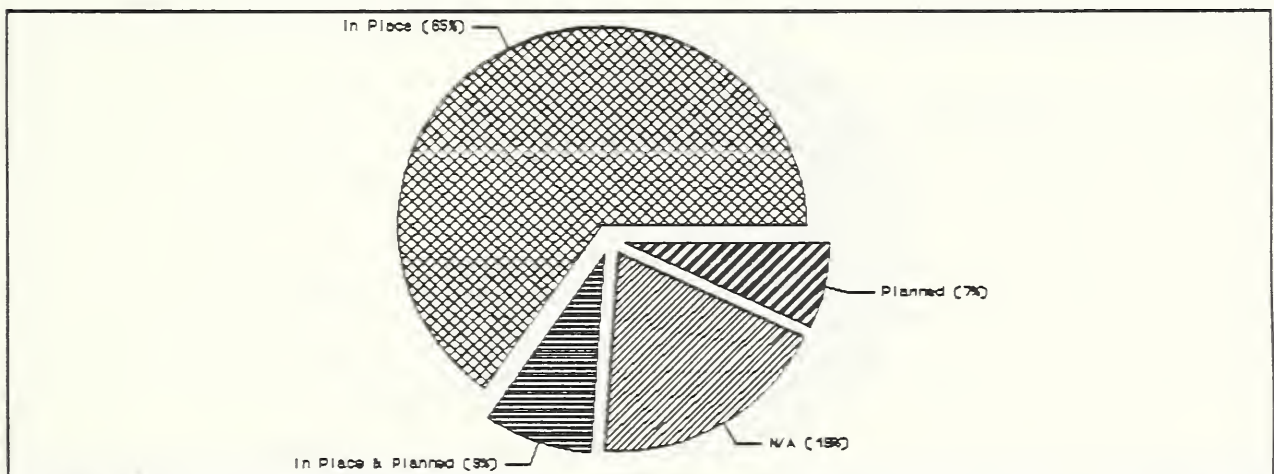
Figure III-28 - Security and Acquisition Specifications-MAS

III-23
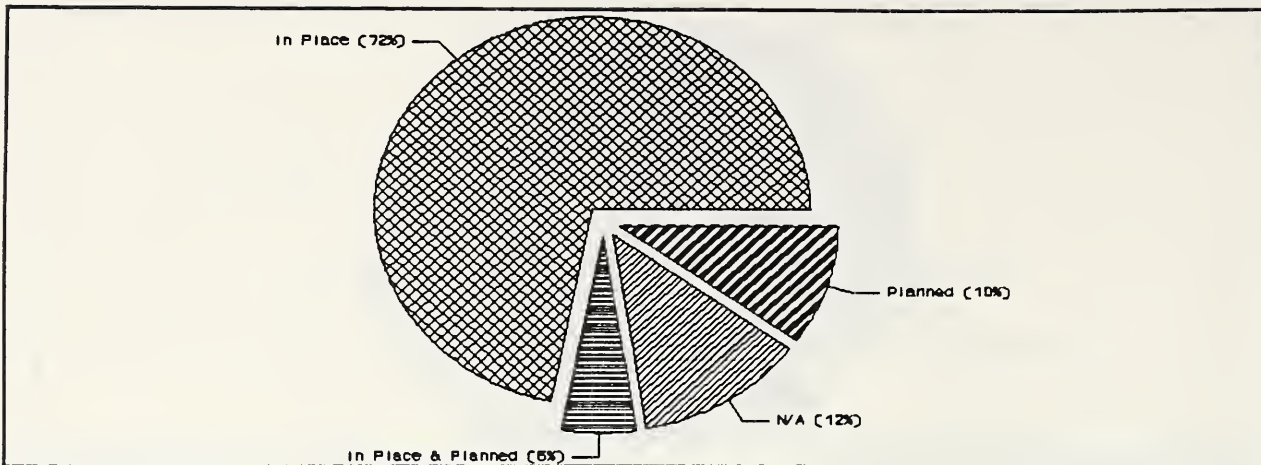
Figure III-29   -   Audit and Variance Detection-MAS
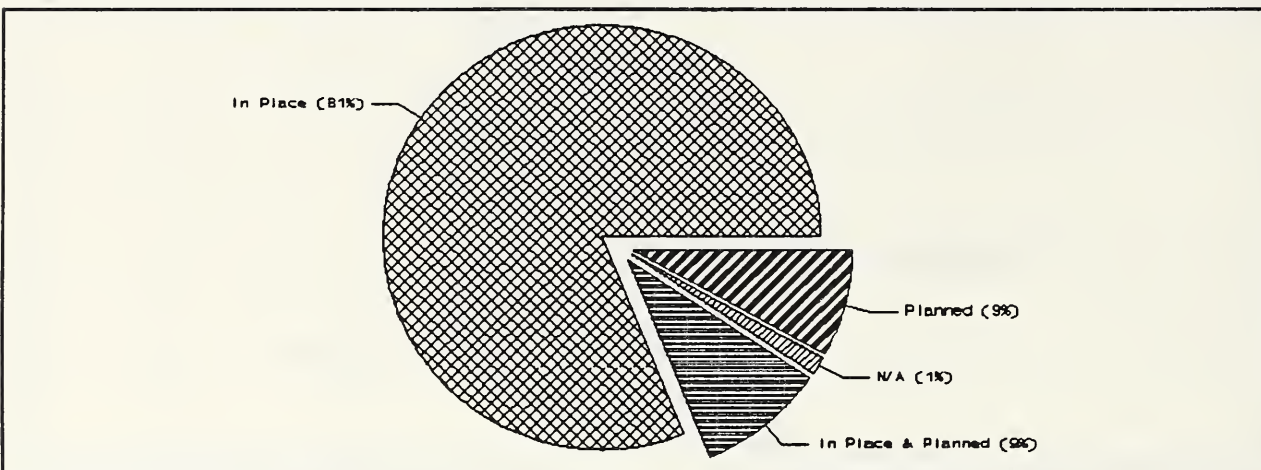
Figure III-30   -   Documentation-MAS
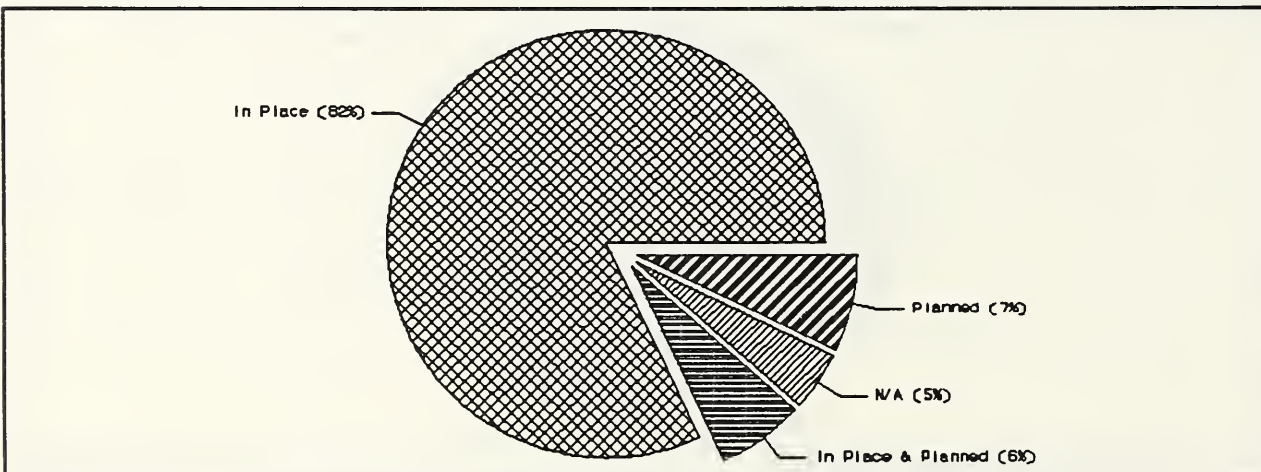
Figure III-31   -   Production, I/O Controls-MAS
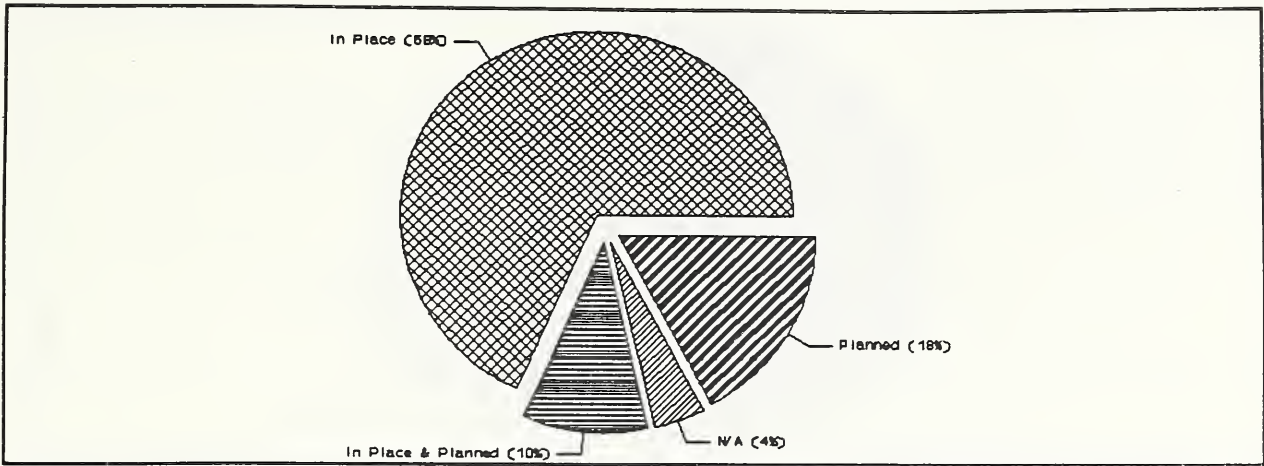
Figure III-32 - Emergency, Backup, & Cont. Planning-MAS
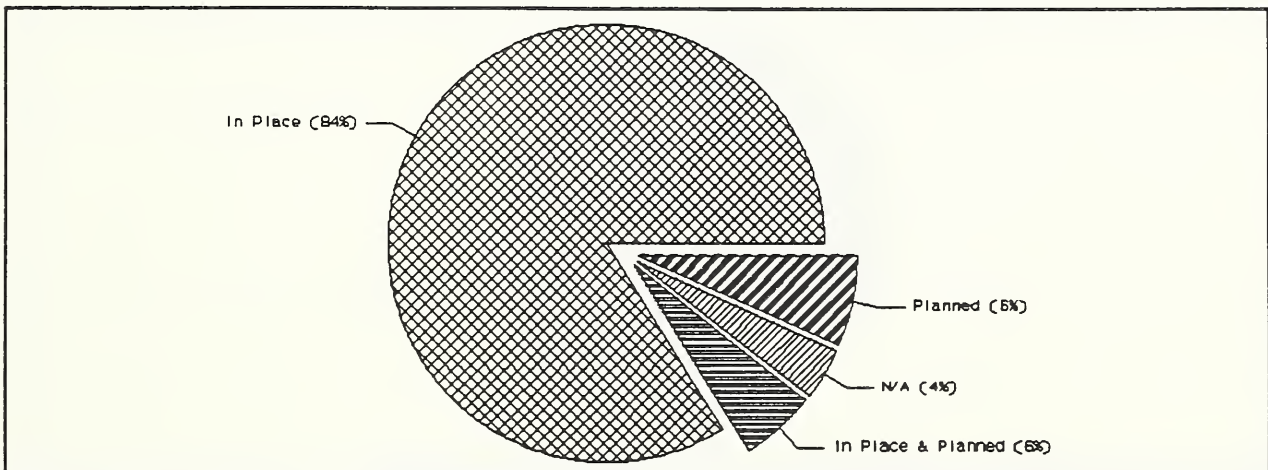
Figure III-33 - System Software and Maintenance-MAS
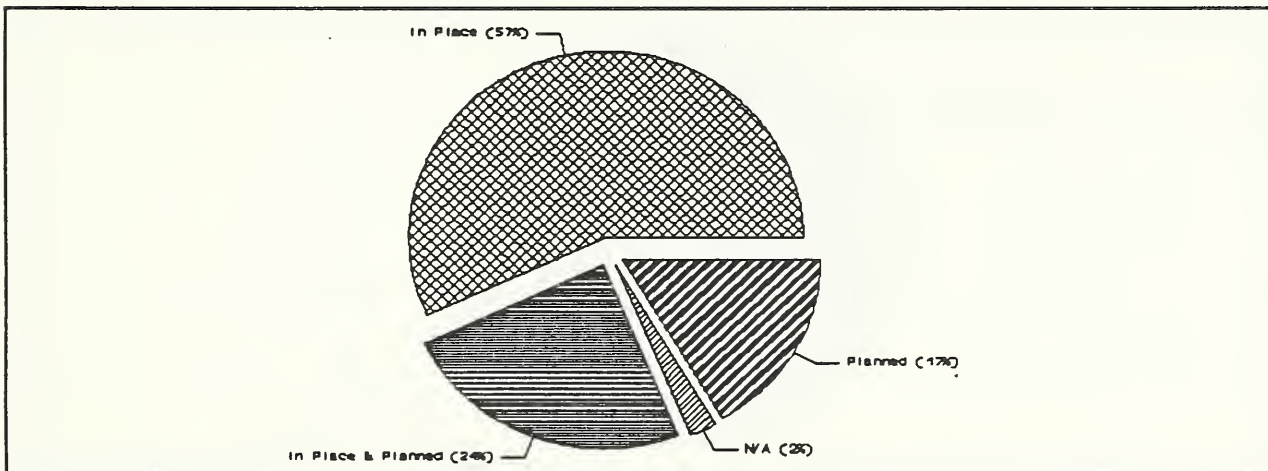
Figure III-34 - Security Awareness and Training-MAS

III-25
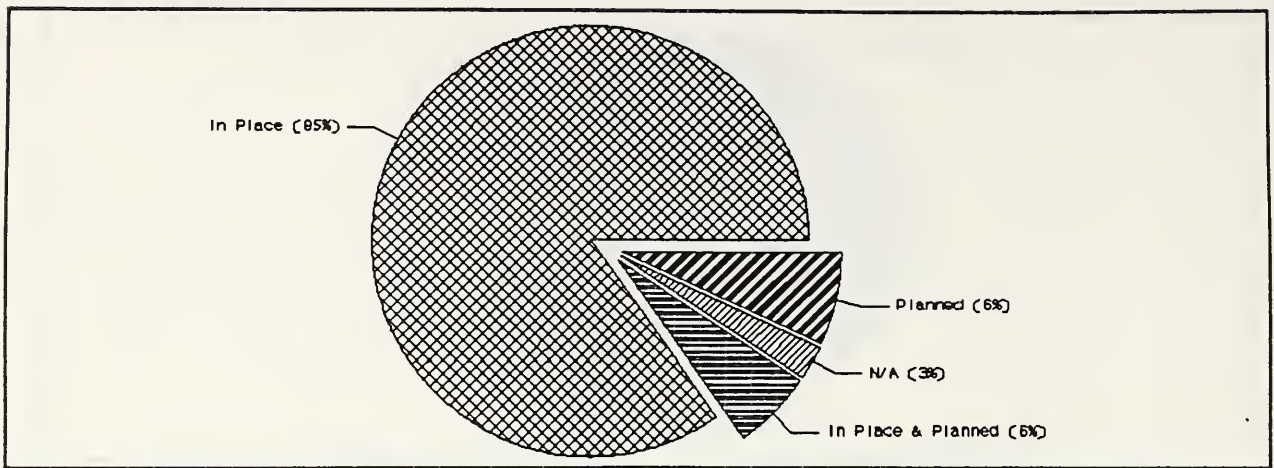
Figure III-35 - Authorization and Access Controls-MAS
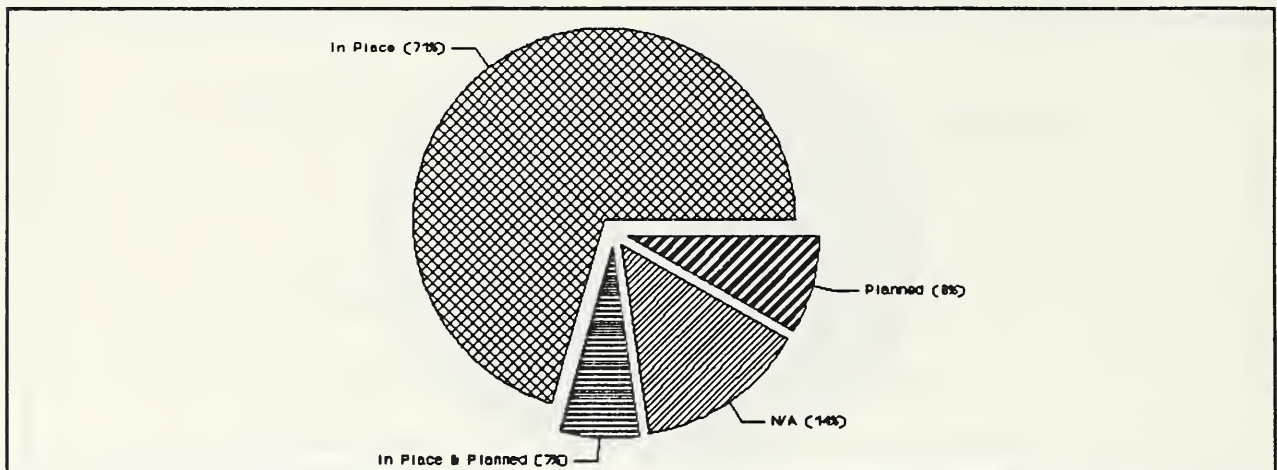
Figure III-36 - Audit Trail Mechanisms-MAS
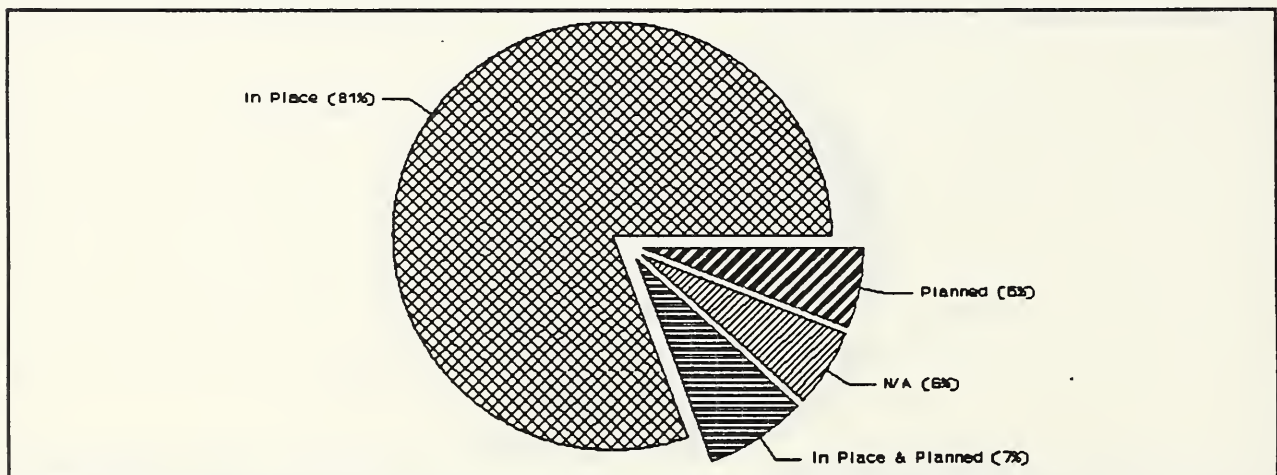
Figure III-37 - Integrity Controls-MAS

III-26
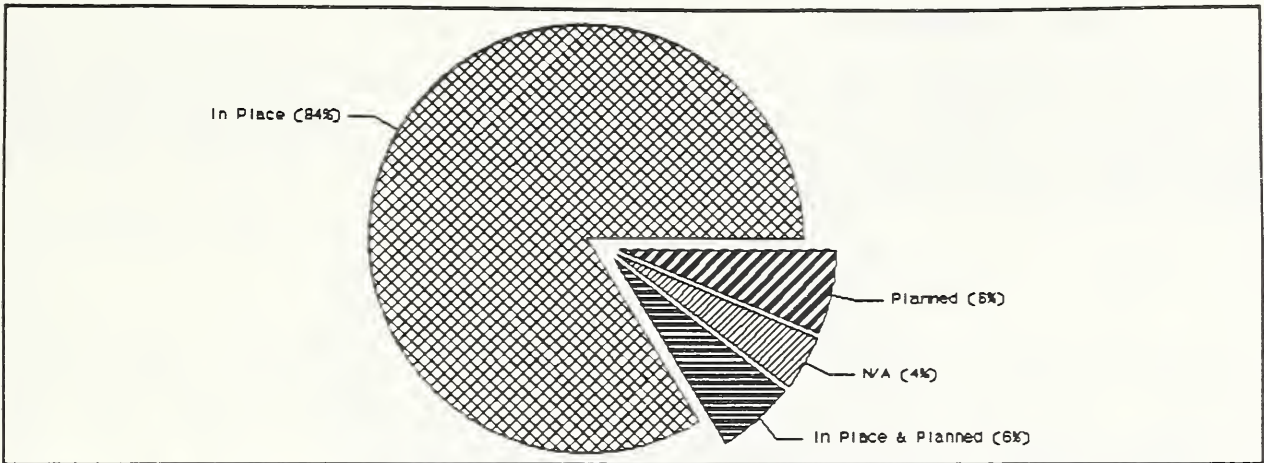
Figure III-38 - User Identification and Authorization-MAS

D.   Data Groupings

This section presents the civilian CSPP data for the basic system identification broken down according to system category and branch of government. The basic system identification fields are: system category and operational status.

1.   System Category

The following Figures III-39 and III-40 present a further breakdown of system category and operational status.   Note: Sixty-five percent of the CSPPs were Major Application Systems (MAS) and 35% of the CSPPs were General ADP Systems (GADPS).
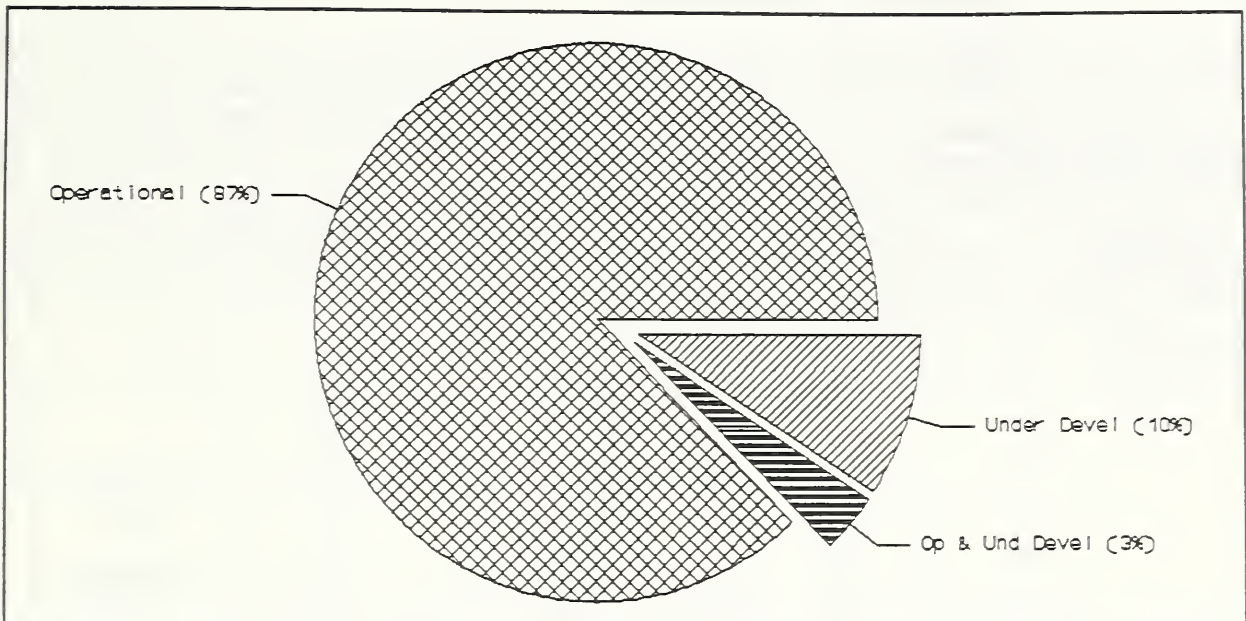
Figure III-39 - Distribution by Operational Status - MAS
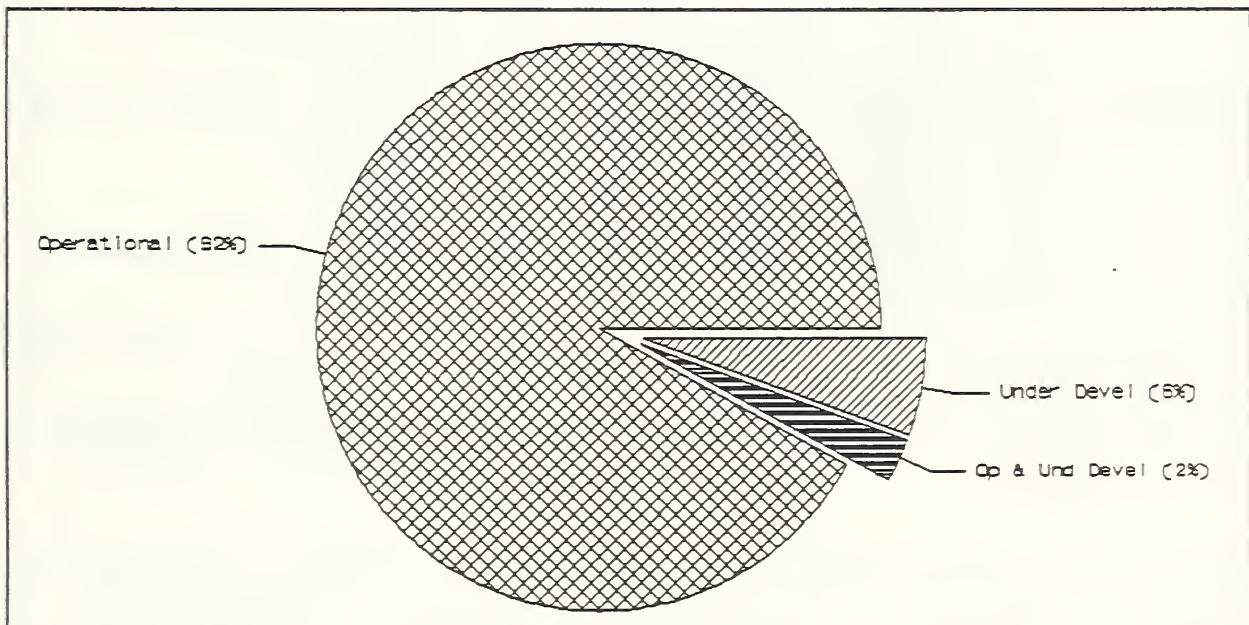
Figure III-40 - Distribution by Operational Status - GADPS

III-29

2.   Branch of Government

Figures III-41 and III-42 and Tables III-12 and III-13 show the CSPP distribution for system category and operational status by branch of government. The executive branch has been separated into cabinet and independent establishments. A list of the agencies in each group and the number of plans in that group is provided in Section III.B.   For ease of comparison the "ALL" grouping represents the overall distribution for all civilian agency plans for each of the respective categories. In these figures, the data is presented as a percentage of each branch.
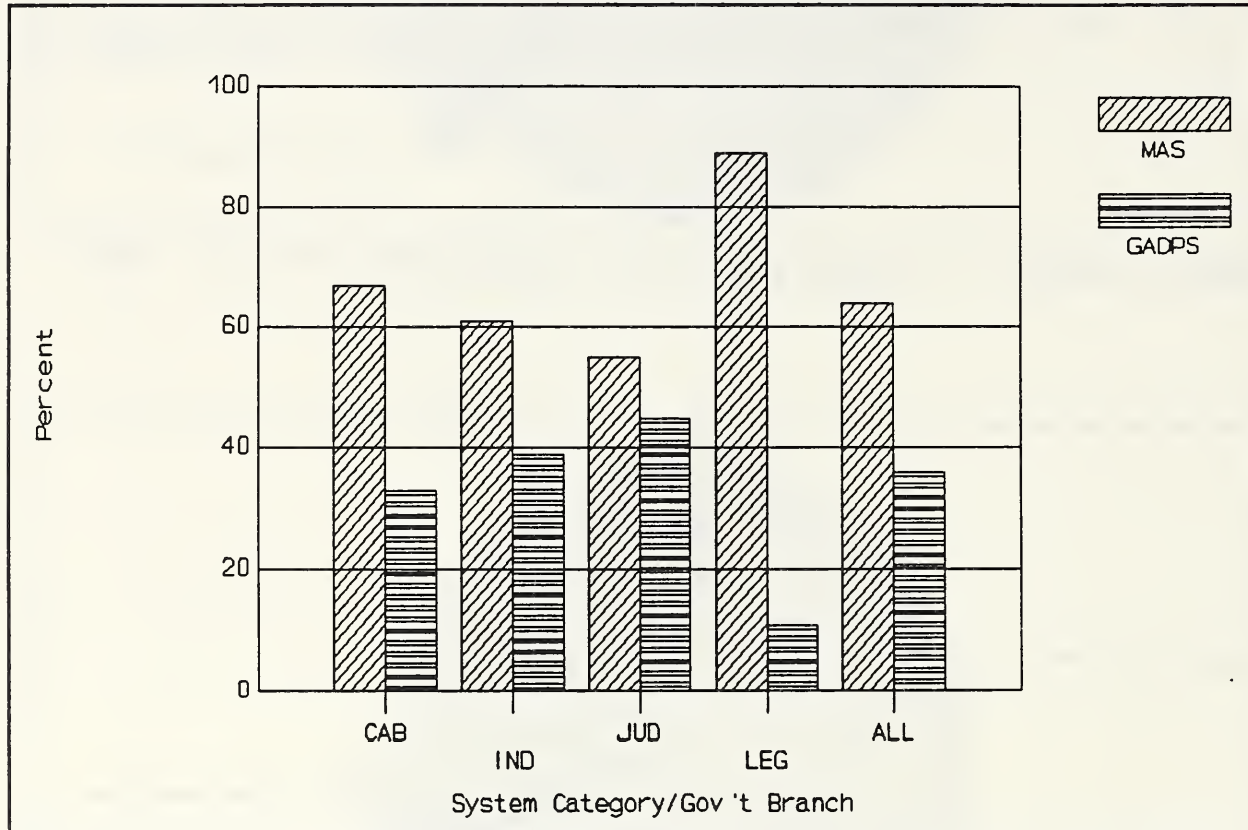
Figure III-41 - Distribution by System Category & Branch

SYSTEM CATEGORY	CABINET	INDEPENDENT	JUDICIAL	LEGISLATIVE	ALL
MAS	67%	61%	55%	89%	65%
GADPS	33%	39%	45%	11%	35%

Table III-12 - Distribution by System Category & Branch
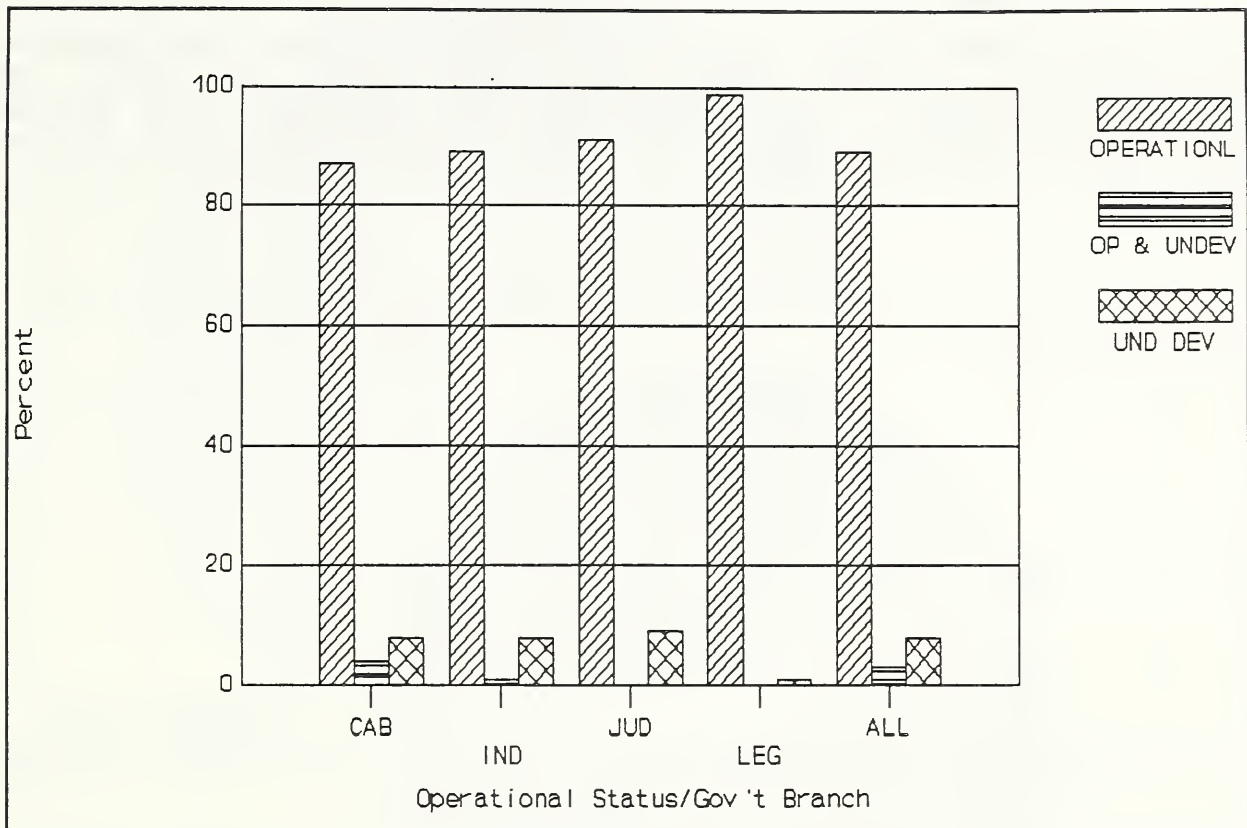
Figure III-42 - Distribution by Operational Status & Branch

OPERATIONAL STATUS	CABINET	INDEPENDENT	JUDICIAL	LEGISLATIVE	ALL
OPERATIONAL	87%	89%	91%	99%	89%
OP & UND DEV	4%	1%	0%	0%	3%
UND DEV	8%	8%	9%	1%	8%

Table III-13 - Distribution by Operational Status & Branch

E.   Department of Defense Plans

Figures III-43 and III-44 and Table III-14 show the distribution of the later 438 DoD submissions, which included 27,937 plans. As explained in Section II.D, Department of Defense CSPP Review Process, more detailed data on the DoD submissions could not be maintained.
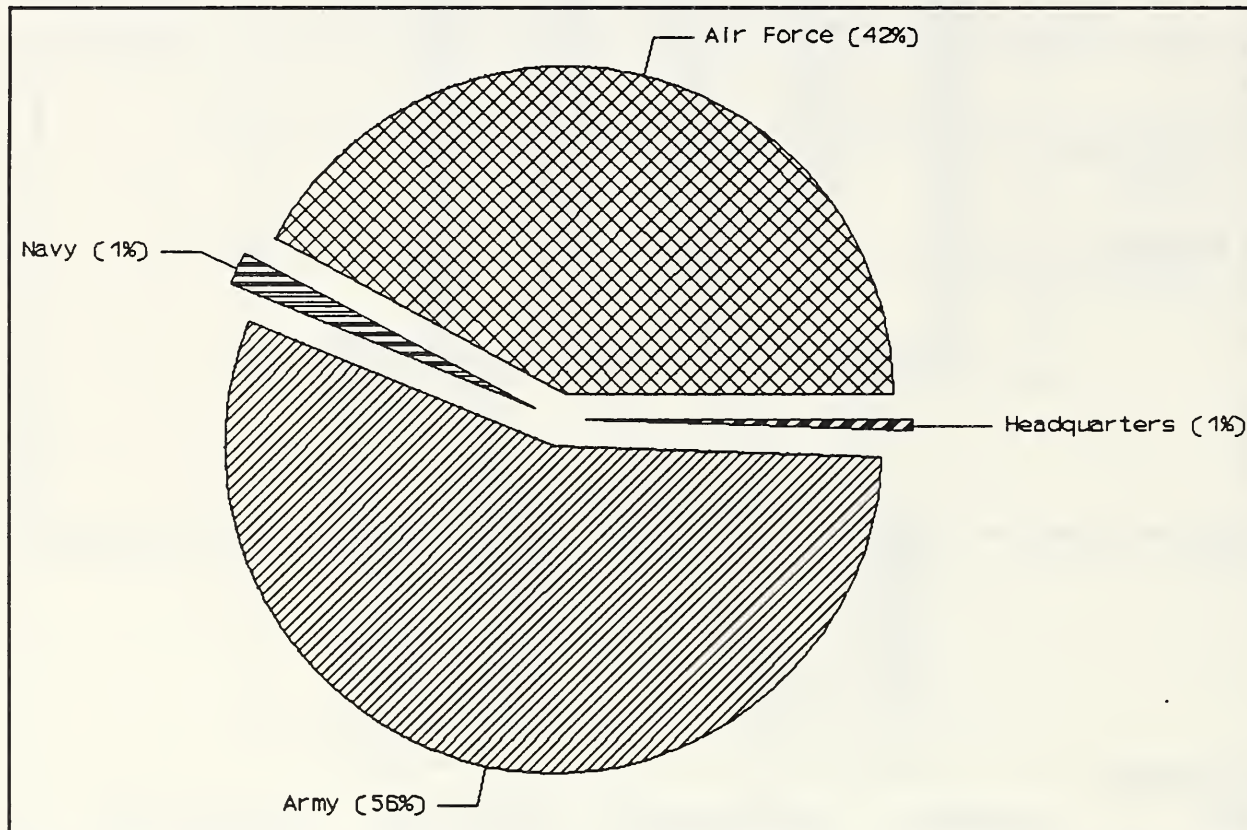
Figure III-43   -   Distribution of Plans by DoD Organizations
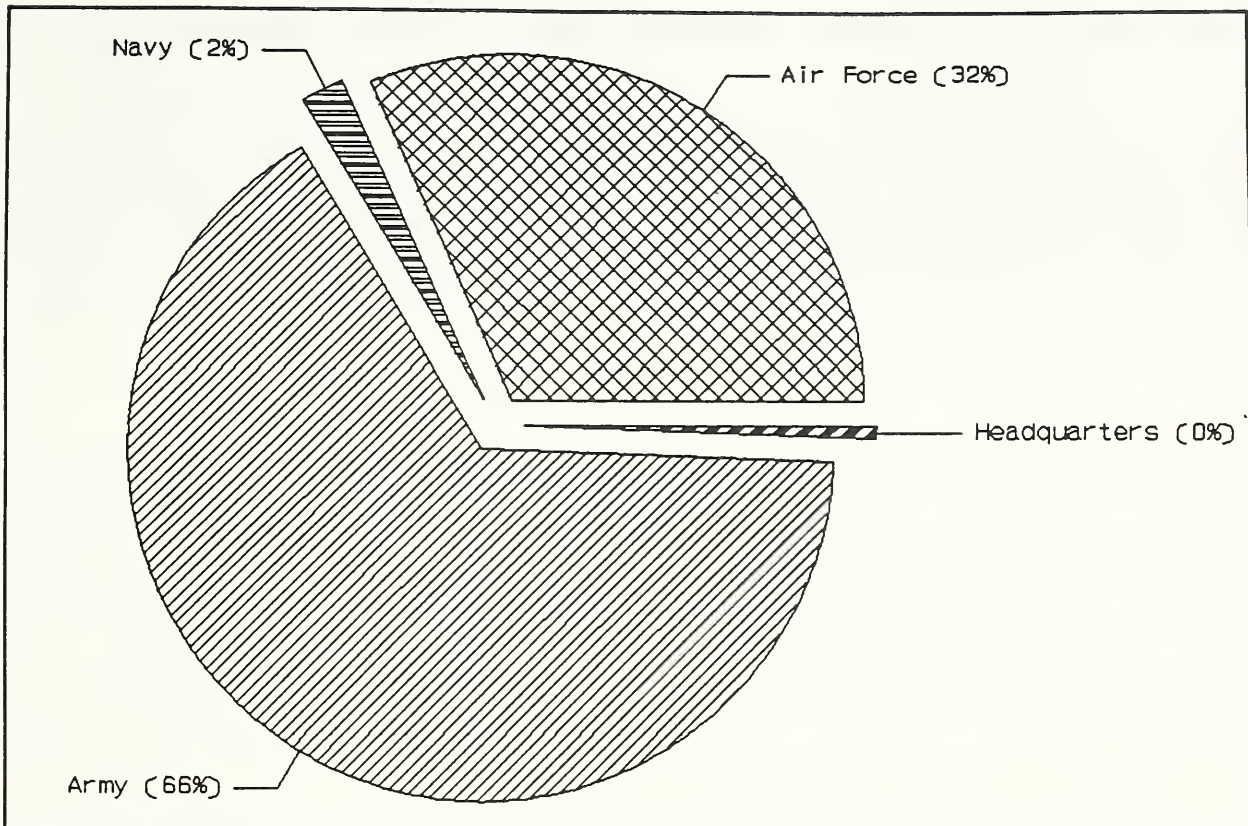
Figure III-44 – Distribution of Submissions by DoD Organizations

| ORGANIZATION | PLANS | | SUBMISSIONS | |
	Number	Percentage	Number	Percentage
AIR FORCE	11,869	42	139	32
ARMY	15,570	56	288	66
NAVY	395	1	9	2
HEADQUARTERS	103	<1	2	<1
TOTAL	27,937	100	438	100

Table III-14 – Distribution of Plans by DoD Organizations

IV. OBSERVATIONS, COMMENTS, AND LESSONS LEARNED - CIVILIAN AGENCY PLANS

The following are observations about the submitted plans and the CSPP review. These include comments made by the review team to the respondents and their agencies. Because the DoD submissions consisted mainly of accreditation documentation prepared for other purposes, the remarks below are based primarily, but not exclusively, on civilian agency submissions.

A. A Learning Process

The preparation and review of the CSPPs unquestionably involved a learning process for all concerned. Large numbers of plans appeared to represent "good faith" efforts, although a small yet noticeable number did not. However, even the good faith efforts did not necessarily produce fully satisfactory computer security plans. In retrospect, the instructions to the respondents should have included the rationale for the requested information, or provided examples, or made clearer what was expected in terms of amounts and levels of detail.

In some instances, respondents answered questions directly, but the questions, and thus the answers, were open to wide interpretation. One example was the question on whether a formal risk analysis was performed. OMB Bulletin 88-16 did not describe what is meant by a formal vs. an informal risk analysis. Each of the control measures in the bulletin was similarly open to interpretation both as to the meaning of the control and variations in its use under different operating environments. For instance, production and I/O controls in a mainframe environment may be quite different from those in a personal computer office environment.

The review team worked with what it was given. It was, therefore, only able to comment on the "goodness" of the plans "as submitted." It was unable to objectively judge how well the plans are being implemented, or the effectiveness of the reported protections. It is clear that better ways need to be developed to describe and correlate computer security plans with effective implementation and cost-effective controls.

B. Consistency/Uniformity and Agency-Level Involvement

There was a decided lack of uniformity among and within agencies regarding a basic understanding of computer security planning issues and of agency and federal policies and requirements. Wide variations were noted in substance, format, completeness, consistency, and compliance with OMB Bulletin 88-16. In some

cases, these variations brought into question whether there was agencywide guidance on the preparation of the plans or agencywide review of the transmitted documents. The variations may also be indicative of differing interpretations of the type and amount of detail required, as noted in the preceding section. The variations may also reflect differences in the degree of diligence with which the effort was approached. In general, the review team noted considerably more uniformity at the service, bureau, or subagency level.

C. Multiple Perspectives and Involvement

One of the hopes of the review team was that the plans would reflect the joint involvement of ADP, computer security, and, significantly, applications communities in computer security planning. While application end users and management may not have technical computer or computer security expertise, they know what information needs to be protected and the reasons for the protection requirements. It was disappointing to the review team that this joint involvement did not happen to the degree envisioned, or at least was not reflected in the plans. It is clear from the submissions that more user and management involvement in computer security planning is necessary. Further, it is apparent that increased cooperative effort is needed in this area among those providing guidance and direction, and those responsible for implementing computer security at the system, subagency, and agency levels.

One example of this lack of multiple perspective is a plan for a central mainframe. The plan described this system as a general support system with no special types of sensitive data. However, other plans from the same agency described applications that ran on the mainframe, including a personnel system subject to the Privacy Act. The agency's mainframe planner did not seem to have coordinated with the application managers.

D. Compliance with OMB Bulletin 88-16

In general, most of the agency submissions were compliant with OMB Bulletin 88-16 by addressing, to some degree, the minimal level of information requested by the bulletin. It is encouraging that many of the controls to protect sensitive systems were reported to be already in place or planned, and appeared to be consistent with the identified system functions, environment, and security needs. However, some respondents appeared to have just "checked the boxes" addressing control measures, thereby presenting a falsely optimistic picture.

E.   Completeness of the Submission

The Act left to the agency's discretion whether each of its systems
was or was not sensitive. The review team was concerned that for
some agency submissions the plans appeared to represent isolated
systems rather than the full range of systems subject to the
Computer Security Act and OMB Bulletin 88-16. Some submissions
were not as complete as one might expect. The review team deferred
to the agencies and OMB the issue of reexamining and reevaluating
whether all of an organization's sensitive systems were
appropriately identified and reported on, and typically did not
comment on this area.

F.   Level of Aggregation

OMB Bulletin 88-16 permitted agencies to aggregate groups of
systems having sufficiently similar characteristics and security
requirements, allowing them to be managed and reportable as a
single system. The review team felt that many respondents made
appropriate use of this allowance. However, there were
aggregations reported with which the review team did not agree, and
others that the review team felt were not within the "spirit" of
the provision. These instances raised questions for the review
team regarding appropriate aggregation and the appropriate
definition or "boundaries" of a "system" for computer security
planning purposes.

The review team encountered "point of view" problems with this
category. Is a mainframe complex running several applications to
be considered an aggregation of major applications, an aggregation
of several mainframes or a single ADP support facility? Similar
questions can be raised for very large applications that encompass
diverse hardware and sub-applications. Various points of view
caused agencies to report quite differently on systems that were
essentially alike.

G.   Agency Overviews and Agencywide Computer Security
Framework and Policy

An overview can be a useful tool in communicating, both internally
and externally, agencywide security measures and concerns.
Overviews typically address: agencywide computer security policies,
procedures, standards, and requirements; the agencywide computer
security and privacy program structure and operations; agencywide
computer security and privacy controls and protections which may
not be reflected in the agency plans for individual systems;
agency-level concerns about the plan submission process and
requirements; and agency-level needs for guidance, standards, and

technology. Such documents can clarify how the individual elements contribute to a unified agency approach to computer security.

Most agencies did not provide an overview of their computer security and privacy program. Such documents would have been helpful to the review team in better understanding the agency submissions. In their absence, it was often unclear whether an agencywide computer security policy had been issued. Also unclear ~~was~~ were the meanings of acronyms and ratings and other codes that were sometimes used throughout a submission.

H.   Do the Plans Themselves Represent a Vulnerability?

The question arose as to whether the plans, which reported on security concerns, themselves represented a vulnerability. The review team felt that this issue was adequately addressed through the combination of: 1) the instructions in OMB Bulletin 88-16 regarding the fact that the submitted plan was "not intended to be a detailed technical description of system content, risks, or security mechanisms"; and 2) the administrative and review procedures which placed a premium on the confidentiality of the plans. In the few instances where the review team felt that there was potential vulnerability, this was noted in the review and comments.

I.   Comprehensiveness of System Description

Although over 60 percent of the plans provided adequate system and environment descriptions, for many plans this was a weak area. While 79 percent of the plans identified hardware, 60 percent did not identify application software or types of system software, and 13 percent did not describe their systems in mission-related or functional terms.   While some aspects of the environment descriptions were sufficient, 30 percent of the plans did not present descriptions of the user community. The environment description should include some indication of the level of user sophistication and information on the physical, operational, and technical environment of the system. It should additionally cover special circumstances, such as use of a data processing center outside the agency's control, or whether the center supports a substantial external customer base, and whether the user community includes individuals external to the government or government contractors.   These factors may be extremely important in determining the nature and relevancy of implemented and planned security controls.

Examples of problems in this area included general descriptions such as "engineering system," and environment descriptions such as

"the model XYZ computer is kept in a computer room with air conditioning and raised flooring." While these descriptions provide information about the system, they do not adequately address the nature of the system in the context of their mission and their operating environment.

J. System and Information Sensitivity

Based on observations made during the review process many agencies had great difficulty and struggled with describing their security needs of both their system and their information sensitivity. Descriptions of information sensitivity should include a general description of the value of the information; the potential damage which might occur through error, unauthorized disclosure or modification, or unavailability; and a statement of the generic threats to which the system or information may be vulnerable. It is the combination of the system's functions, environment, and sensitivity which permits management to determine the requirements for and evaluate the relevancy of implemented and planned security controls. Agencies' problems in describing their system and information sensitivity revolved around two areas, incomplete descriptions and overemphasis on confidentiality.

1. Incomplete Descriptions

The first area was a lack of description. Forty-eight percent of the plans either did not address all three protection requirements of confidentiality, integrity, or availability; or adequate explanations of reported protection requirements were not provided. This was especially the case when a plan only indicated that the system contained "Privacy Act" or "financial" data. An understanding of the needs for protection is essential to determining the proper controls to implement.

2. Overemphasis on Confidentiality

The second area of agency difficulty in describing their system and information sensitivity was confusion within the descriptions. A number of plans confused or equated "sensitivity" as meaning only "confidentiality." Some plans expressed the notion that unless there is a confidentiality or privacy requirement (as opposed to requirements for integrity and availability), the system is not sensitive. An example of this is a plan for a payroll system which stated that confidentiality was the primary requirement and integrity and availability were secondary or minimal. While this may be the actual protection requirements hierarchy for this system, the "normal" payroll system strongly emphasizes availability. Given the powerful monetary incentive, the protection of payroll systems from fraud is also "normally" a very

important requirement. The descriptions from that plan provided no explanation of the ranking.

Table IV-1 compares the protection requirements as stated in the plans with the type of information processed. The levels for reporting the protection requirements were: Primary, Secondary, and Minimal (including Not applicable). Although the related descriptions of many plans do not adequately address information sensitivity, the table shows that overall, that a significant percentage (84, 95, 92) identified confidentiality, integrity, and availability (respectively) as being either a primary or secondary. Protection requirements reported for financial systems, mission critical systems, and systems that contain Privacy Act or proprietary data are also presented for comparison.

(Note: The numbers are given in percentages. The items in the table are not mutually exclusive. A payroll system could show up as both a financial system and a Privacy Act system. In some instances the sum of the percentages for a protection requirement/type of information combination does not add up to 100 percent due to rounding.)

TYPE OF INFO.	CONFIDENTIALITY			INTEGRITY (Percentage)			AVAILABILITY		
	PRI	SEC	MIN	PRI	SEC	MIN	PRI	SEC	MIN
ALL PLANS	66	18	16	80	15	5	66	26	8
FINANCIAL	73	14	12	89	7	2	69	26	3
MISSION CRITICAL	59	20	20	80	14	4	71	26	2
PRIVACY	83	10	6	83	11	5	65	26	8
PROPRIE- TARY	77	17	5	81	12	5	78	12	8

TABLE IV-1 - Percent Comparison of Protection Requirements and Type of Information Processed

K.   Risk Assessment

Forty-four percent of the plans reported that formal risk assessments had been performed. Others, however, reported that no risk assessment had been done, and some even indicated that a risk assessment was not applicable for their systems. In general, the plans did not communicate a clear understanding and appreciation of the significance of risk assessment and risk management activities in computer security planning.

As noted in Section IV.A, A Learning Process, there may have been some confusion over OMB Bulletin 88-16's definition of a formal risk assessment. The review team noted that, in many cases, the benefits of more structured risk assessments might be worth considering. A formal, fully structured risk analysis might consist of identifying assets; determining vulnerabilities; estimating the likelihood of exploitation; computing expected annual loss; surveying applicable controls and their costs; and projecting the annual savings resulting from the controls. OMB Circular A-130 requires periodic review and recertification of sensitive applications and periodic risk analysis for "information technology installations."

One particular problem the review team noted was an agency tendency to think of risk analysis as something that is done after

system development is complete. At least one entire subagency's plans reported that a risk assessment was planned to follow system testing.

L.   Training and Awareness

Respondents reported wide variation in their computer security training and awareness programs. Some plans reported that computer security awareness and training measures were in place or planned, but indicated that the agency would provide training only to computer system personnel, security personnel, or some other limited group within the organization. Similarly, only a very limited number of plans specifically reported that training was received by application managers, whose appreciation of computer security is particularly needed. (Note: OMB Bulletin 88-16 did not require plans to be explicit as to who received the training.) The Act, as well as good computer security management practice, requires security awareness and training for all employees involved in the design, management, development, operation, or use of a federal computer system. This must include periodic computer security awareness and skills training. A fully developed training and awareness program can be a cornerstone for an organization's effective computer security program. In general, while less that 3 percent of the plans did not report these as either in place or planned, there did not seem to be a full appreciation of computer security awareness and training.

M.   Applicable Laws, Regulations, and Guidance

OMB Bulletin 88-16 describes applicable laws and regulations as those documents that "establish specific requirements for confidentiality [and integrity and availability] of information in the system," and applicable guidance as "standards and other guidance used in the design, implementation, or operation of the protective measures used in the system..." Most plans included many references under either or both of these categories. This indicated a good level of awareness of federal and agency policy and directives. However, numerous plans showed little awareness of agencywide direction in this area. There appeared to be confusion as to whether agency documents were required to be referenced. The Privacy Act was very widely referenced. However, other plans which could have referenced the Privacy Act, or OMB Circular A-130, or agency policy implementing these directives, did not do so. A number of plans referred only to "standard industry practice" or "federal guidance." See Appendices G and H for listings of applicable laws and regulations and applicable guidance, respectively, reported by the CSPPs.

N.   Security Controls

A significant majority of the plans reported that many, or all, security controls were in place or planned. Two percent of the plans did not adequately address the system control measures or their status, as specified in OMB Bulletin 88-16. Additionally, a number of plans suggested an imperfect understanding of the meaning and effective use of the controls. Many plans for operational systems stated that development controls were not applicable. Twenty-nine percent of the plans stated that certification and accreditation were not applicable. When the plans provided narrative about the controls, it was often apparent that the controls were not understood. Many of the plans confused audit and variance detection, an operational control, with audit trails and journaling, a technical control. Since most of the plans simply checked the boxes to indicate the status of the controls (as opposed to providing narrative description), the review team was unable to determine what the plan meant by the controls and, therefore, whether the controls were appropriate to system security requirements.

One percent to 14 percent of the plans described one or more of the operational controls to be not applicable. (For example, 14 percent reported audit and variance detection to be not applicable and 7 percent reported production controls to be not applicable. Some plans indicated that one or more technical or one or more development controls were not applicable (4-20 percent and 19-29 percent of the CSPPs, respectively)). While there may be legitimate reasons why some controls may be unnecessary in a given situation, the absence of some controls raises the question as to whether there exists a full appreciation of what the specified controls represent, or their significance. A recommendation frequently made by the review team was that those responsible for the individual plans fully document the in-place controls to facilitate periodic reevaluation, internal audit, and oversight agency review.

O.   Implementation Dates for Planned Controls

OMB Bulletin 88-16 requested that for planned security measures, a general description of the measure and an expected operational date be provided. In general, this was done, but a few plans did not report these for the planned controls identified. Such dates should reflect the system protection requirement priorities of confidentiality, integrity, and availability in terms of primary, secondary, or minimal concern. Where all three system protection requirement categories are considered primary, timely implementation of security controls covering all three categories, although difficult, may be necessary.

P.   Internal Consistency of the Plans

There were apparent internal inconsistencies among the information reported in a number of plans.   This was often seen in the relationship between the stated requirement for confidentiality, integrity, and/or availability, and the reported control measures supporting the requirement were indicated to be not applicable. For example, some plans reported a requirement for confidentiality, but did not report controls to support that requirement.   Another example is when development controls were reported to be not applicable for systems under development.   One agency submitted a plan for a system that appeared to the review team to be sensitive from it description, but the plans reported it to be not sensitive in that confidentiality, integrity, and availability were all not applicable.

Q.   System Boundaries: Telecommunications and Networking, System Interfaces, and Contractors

Many plans described systems that involve some form of interaction with entities outside of the systems' physical, logical, or organizational boundaries.   This included systems in which telecommunications and networking are integral, systems in which data is transferred to or from other organizations, and systems that utilize contractor support or facilities.   Very rarely did these plans present an adequate description of the environments or sensitivities, or a full appreciation of the exposures associated with system boundaries.   (Note that while OMB Bulletin 88-16 was explicit regarding contractor and other systems, it did not specifically address telecommunications and networking and system interfaces.)

This lack of description may reflect a general confusion as to the boundaries and limits of responsibility for a given system. Although OMB Circular A-130 clearly states that an agency is responsible for all automated information systems "whether maintained in-house or commercially," the plans often did not reflect an understanding of how to manage systems which crossed physical, logical, or organizations boundaries.

In a number of instances, the review team urged the plan respondent or agency to include, in any planned risk assessment activity, full consideration of the telecommunications and networking environment and its relationships with other organizations.

R.   Needs and Additional Comments

It was disappointing that only a very few plans took advantage of
the opportunity to provide needs and additional comments. If used
effectively, this section could have been used to indicate any
needs for specific guidance, standards, or other tools to improve
the protection of systems being reported, or the protection of
agency systems, on the whole.

Of the plans received, fewer than 100 reported needs and additional
comments.   Of those responding, the most frequently mentioned
concerns were regarding guidance on computer security training and
the need for policies for sensitive data on microcomputers. Table
IV-2 presents the specific concerns reported.

NEEDS AND ADDITIONAL COMMENTS

CONCERNS	NUMBER
Security training for all users	11
Policies and written procedures for dealing with sensitive data on a microcomputer	11
Funding needed for increased computer security	8
Guidance on responsibilities, duties, and qualifications for a database administrator	7
Government policy covering authentication and accountability of reports	7
Audit process	5
Password control	5
Computer security responsibility defined and delineated	4
Control of data and software coming in from the outside	4
More communication and technical support between the user and the technical people	4
Sample of required security reports and plans, reflecting actual formats and plans	4
User responsibility for a system they have no control over	4
Information on cleaning data from hard disk	3
Automated tool to highlight variances	2
Automated tool for statistical analysis	2
Current security manual rewrite to reflect state-of-the-art in computers and security	2
Electronic storage for eliminating paper	2
Faster response on modification requests	2
Authorized interactive assessment program	2
Database management system	2
System replacement	2
User authentication	2
Procedures for storage of floppy disks with sensitive data	1
Encourage development of hardware, software, and techniques for computer security by vendors	1
Method of finding cost-effective security approaches	1

TABLE IV-2 — Needs and Additional Comments

S. What Was Reported vs. What Was Communicated

As discussed earlier, eighty-four percent of the plans reported confidentiality as a primary or secondary protection requirement, but 95 percent and 92 percent reported integrity or availability as primary or secondary, respectively. However, the review team members did not get the sense of a full appreciation of integrity and availability concerns from the plans themselves. Similarly, although nearly all the plans reported that they had done some sort of risk assessment (formal, other, both) or that they had risk assessment controls in place or planned, the plans, in general, did not communicate a sense that risk assessment was a significant factor in determining security measures or that it was used as an active tool in security planning.

V. OBSERVATIONS, COMMENTS, AND LESSONS LEARNED - DEPARTMENT OF DEFENSE PLANS

A. DoD Compliance with OMB Bulletin 88-16

As previously stated, the DoD submissions did not provide information based on OMB Bulletin 88-16. Generally, the documents did not include a description of the system, its environment, the system protection requirements, or the types of security measures that were in place or planned. While the submissions contained useful information on existing security measures, they basically did not reflect the planning which resulted in these protections. The review team was not always able to determine the confidentiality, integrity, and availability requirements of the systems. Without an understanding of the sensitivity of the system or its data, the review team could not comment on the adequacy of the controls in place or planned.

B. Consistency/Uniformity

Within each submission, there was generally a consistency in the format and content of the documents. For this reason, the review team felt that one response per submission rather than one response per plan was appropriate. Most of the plans included some combination of the following documentation: accreditation requests and/or approvals to operate, risk management reviews, facility security profiles, risk analysis checklists, system description sheets, standard operating procedures, letters of certification, equipment lists, and formal risk analyses. Checklists usually addressed physical controls and procedures, but did not indicate any planning that resulted in the procedures being implemented. In spite of the variety and magnitude of the submissions, the review team reviewed the documents and noted any evidence that might indicate that sensitive information was not afforded the proper protection.

C. Training and Awareness

Most of the DoD plans did not indicate the existence of a security awareness and training program. A few plans indicated that security officers had received training, and a smaller number indicated that security officers had not received training. Since the Computer Security Act specifically mandates security awareness and training, the review team noted such in its response whenever the plans did not explicitly state that initial and periodic computer security training was in place for all users of the system.

D. Applicable Laws, Regulations, and Guidance

The submissions generally displayed an understanding of the DoD computer security regulations such as DoD Reg 5200.28, Army Reg 380-380, Air Force Reg 205-16, and Navy OPNAVINST 5239.1A. Several plans included copies of the base Standard Operating Procedures, which were also reviewed for insight into the base's planning process.

E. Sensitivity/Criticality

Many plans used sensitivity and criticality codes to label the sensitivity of the systems. Several different sets of codes were used, even within the same service. The sensitivity code generally corresponded to need for confidentiality, while the criticality code generally corresponded to the need for availability. While the codes allowed the review team to recognize whether these security requirements were primary, secondary, or minimal, there usually was no further explanation of system sensitivity.

F. Security Controls

Since the DoD submissions did not provide the information requested by OMB Bulletin 88-16, they did not include data concerning most of the system security controls. Due to this lack of information, the review team only made recommendations concerning controls that were noted as not in place when other indications suggested that they may have been necessary. For example, a few plans indicated that the system's data were critical; yet the plans also noted that they had no contingency plans.

G. Telecommunications and Networking

Many personal computers were accredited to operate in a stand-alone mode, but the equipment list would include modems or the plan would reference electronic mail and local area network connections. There was rarely any mention of security controls that are necessary due to telecommunications and networking.

H. Accreditation Consistency

In some cases, there was a lack of consistency between the letters of accreditation and the supporting documents within a submission. In several plans, systems were accredited to run at a designated sensitivity level that was different from the sensitivity of the data described in the system description. Other submissions revealed that systems accredited to process only unclassified

information actually processed "limited" classified data. (See Section V.I, Classified Systems, below.) Within several large submissions, all the accreditation documents were stamped with the same date, usually very close to the date that the plans were sent to the review team, a fact that called into question whether all systems had, in fact, been accredited prior to the submissions.

I.   Classified Systems

While this project reviewed sensitive unclassified system plans, several plans were received for systems that did "limited" classified processing. Security officers apparently treated these systems as unclassified because "no classified data would be stored on the hard disk." These security officers did not indicate an awareness of the possibility that some computer programs store temporary files on the hard disk. Realistically, classified data may be written to the hard disk without their knowledge. Although these files were deleted, the data remains on the hard disk and can be recovered. The review team reported this and recommended that proper sanitization procedures be completed after any classified processing takes place on these systems.

VI. CONCLUSIONS

A.   Conclusion: Many Positive Signs,......

While the review team found many areas where improvements can be
made in protecting federal information systems and where planning
to accomplish this needs to be done, the team was highly encouraged
by many positive signs.   Aside from DoD submissions, the CSPPs
basically conformed with OMB Bulletin 88-16. Most controls needed
to protect sensitive systems were reported to be already in place
or planned, and these appeared to be consistent with identified
system functions, environment, and security needs.   Ninety-eight
percent of the plans reported security awareness and training as
in place or planned. Similarly ninety-seven percent reported risk
assessment activity as in place or planned.   Likewise, a high
percentage of plans reported requirements for confidentiality,
integrity, and availability as primary or secondary (84.0 percent,
94.9 percent, and 92.4 percent, respectively). This indicated some
consideration of these requirements, although not necessarily a
full understanding of them.

B.   Conclusion: .....But Some Areas for Improvement

Despite the above positive signs, it appeared that some respondents
just "checked the boxes," perhaps presenting a falsely optimistic
picture in some areas.   Many agencies appeared to report on
isolated systems rather than all the agency programs that might be
subject to the Act and OMB Bulletin 88-16.   In some cases, it was
questionable whether there was agencywide guidance on the
preparation of the plans or agency review of the submission. Also
unclear is the extent of agency-level computer security policy and
guidance.   Further, most plans did not reflect the joint
involvement of ADP, computer security, and applications communities
in computer security planning.

Significantly, the plans rarely addressed security concerns
regarding telecommunications and networking, interfaces with other
systems, and the use of contractors and contractor facilities.
This may reflect a general confusion as to the boundaries and
limits of responsibility for a given system.   Many plans equated
sensitivity only with privacy or confidentiality, and did not fully
address requirements for integrity and availability. Most plans,
although reporting risk assessments, did not fully communicate an
appreciation of the role of risk management activities in computer
security planning. Although most plans reported computer security
awareness and training, many did not indicate that all applicable
employees received periodic training.   Additionally, the
relationship and importance of incorporating computer security as
an integral part of systems being developed and acquired was not

clearly communicated to the review team through the plans.

It is unclear whether the plans submitted to NIST and NSA under OMB Bulletin 88-16 were true computer security planning instruments, or only artifacts produced to satisfy an external submission requirement. It is hoped that, regardless, the exercise served to increase the level of awareness regarding federal computer security planning. Some CSPPs clearly communicated that those who prepared them knew what they were doing and "had their act together." Other plans, whether or not they said the right words or checked the right boxes, did not promote a similar level of confidence.

The review team concluded that there was no such thing as a model plan. Legitimate, situation-dependent considerations led to many different implementations and strategies. Similarly, it was clear that "good" plans did not have to report every control in place or planned, but rather only needed to demonstrate that due consideration had been given in addressing all of a system's protection requirements.

C. Recommendations for Agencies

Based on the needs that became apparent during the plan review, the review team recommends the following:

1) Agency management should ensure that computer security has the highest level of management involvement. This involvement is also important in the computer security planning process. Computer security benefits from the multiple perspectives of and input from agency IRM, computer security, and functional, user, and applications personnel.

2) Agency management should identify and describe the security needs of their systems which contain sensitive information.

3) Agency management should recognize the importance of computer security and its required planning. This recognition should be aggressively communicated to their staffs, perhaps using their computer security and awareness training programs as one of the vehicles.

4) Agencies should incorporate computer security planning with other information systems planning activities through agency policies and procedures regarding system development and acquisition. Development controls, as identified in OMB Bulletin 88-16, (including those security controls related to acquisitions) as a group

represented a lower level of awareness and implementation among the reported plans. (Note that for each of development controls, 19 percent to 29 percent of the CSPPs reported one or more as not applicable.)

5) Agencies should consider the protection requirements for integrity and availability on an equal basis with that of confidentiality.

6) Agencies should assess risks and select and implement realistic controls throughout the system life cycle. This involves awareness of technology changes with regard system hardware and software. This awareness also requires a knowledge of new technology and new methods for protecting and recovering from system threats. Agencies also should fully document in-place controls to ease periodic reevaluation, internal audit, and oversight agency review.

7) Agencies should implement certification and accreditation programs. There is a lack of awareness of FIPS PUB 102, Guideline for Computer Security Certification and Accreditation. A knowledge of certification requirements in OMB Circular A-130 is not clear. Agencies may use OMB Circular A-130 as the basis for these programs.

8) Agencies should clarify the boundaries and limits of responsibility for each system, and should include, in any planned risk assessment activity, full consideration of the telecommunications and networking environment and relationships with contractors and other organizations.

9) Agencies should stress security awareness and training for their employees. This includes all employees involved in the design, management, development, operation, or use of federal computer systems containing sensitive information.

10) Agencies should develop computer security policy and operative guidance. Such policy and guidance should fully reflect and comprehensively address an encompassing view of computer security. The Computer Security Act, OMB Circular A-130, and OMB Bulletins 88-16 and 89-17, "Federal Information Systems and Technology Planning," and their successors all contain this view. The policy should directly address the full scope of computer security planning and risk management activities. It must incorporate an application system perspective, and give more detailed consideration to confidentiality, integrity, and availability protection requirements.

D.   NIST Plans

Building upon the computer security planning activities begun under the Act and OMB Bulletin 88-16, NIST is evolving a strategy for providing guidance to federal agencies in identifying and protecting sensitive information systems.   This strategy shifts emphasis to the implementation of computer security plans, particularly those developed under OMB Bulletin 88-16. It provides for visits by OMB, NIST, and NSA staff. This group will provide direct comments, advice, and technical assistance relative to the agency's implementation of the Act.   Among the items to be discussed at these meetings will be the agencies' responses to OMB Bulletin 89-17.   This bulletin required agencies to include a summary of their security plans in the agencies's five-year information technology plans.   See Appendix E for a copy of OMB Bulletin 89-17.

In addition to the agency visits described above, NIST has initiated the following computer security projects to help agencies more easily and effectively comply with the Computer Security Act:

1)   NIST will develop standardized specifications and language for federal government computer security services contracts. Agencies and government contractors would be able to use these specifications as a basis for a common understanding of each described activity. The existence of the standard specifications and language will promote easier access to more consistent, quality computer security services.

2)   NIST will develop a guidance document on computer security in the ADP procurement cycle. This will include security during procurement planning, the use of risk analysis in specification development, methods to procure security features and assurances, and clauses that can be used to protect the government from contractor error or negligence.

3)   NIST has recently published guidance on the use of Trusted Systems.

4)   NIST will develop guidance on computer security planning.

5)   NIST has developed, and will continue to operate, a computer incident response center in order to address viruses, worms, and other malicious software attacks.

6)   NIST will support and coordinate computer security

resource and response centers nationwide.

7) NIST will enhance and operate the NCSL Computer Security Bulletin Board System.

8) NIST will operate the NIST/NSA Risk Management Laboratory and prepare further guidelines on risk management.

9) NIST will develop guidance and recommendations on assuring information integrity in computer systems. (See Appendix I for references on NIST Special Publications 500-160 and 500-168 for reports on NIST sponsored data integrity workshops. Also see Appendix E for OMB Circular 89-17.)

In addition to the above plans, NIST has already developed a number of guidelines and other resources to help federal managers secure their computer systems. Significant among these are three awareness guides addressing the needs of executives, managers, and users, and a training guide which identifies federal employees who require training and recommends what training they should receive. See Section I.E, Additional Sources of Information, for information on NIST publications, the NCSL Computer Security Bulletin Board System, the NIST/NSA Risk Management Laboratory, and NSA's National Computer Security Center (NCSC) Bulletin Board on DOCKMASTER. Also see Appendix I, References, for other sources of information on computer security.

E. Lessons and Benefits

Federal managers have specific computer security requirements that are similar to their counterparts in the private sector. We believe that private sector organizations can learn and benefit from the federal experience in implementing the Computer Security Act. In both environments, a vigorous computer security awareness program is important at all levels in the organization. Also, in both environments, the active involvement of user, management, ADP, and computer security communities in computer security planning could help end some of the existing and potential barriers to effective computer security. Such collective involvement would also help ensure cost-effective control measures commensurate with system function, system sensitivity, security requirements, and analyzed and considered risks.

F. Some Closing Thoughts

Agencies need to be aware of developments taking place in the national and international standards arena regarding system interoperability and data interchange. These developments will

likely impact information system product availability, protection requirements, and protection alternatives as agencies do their near-, mid-, and long-term IRM and computer security planning. The Government Open Systems Interconnection Profile (GOSIP), NIST FIPS PUB 146, and the development of security standards for the Portable Operating System Interface for Computer Environments (POSIX) may be of help in addressing some of these needs.

Finally, because agency awareness of problems is fundamental to the solution, this exercise has been valuable. Computer security officers and IRM officials have indicated that the CSPP preparation and review activity has raised the level of awareness about computer security in all parts of their organizations. These activities have made it easier for them to promote computer security. (See Appendix J, Examples of Agency Reactions to CSPP Reviews.) The CSPP review project significantly raised the level of federal awareness about the protection of sensitive information and the importance of computer security planning. In the final analysis, this contribution may be among the most meaningful results of the project.

LIST OF APPENDICES

A.   THE COMPUTER SECURITY ACT
B.   OMB CIRCULAR A-130, APPENDIX III
C.   OMB BULLETIN 88-16
D.   CSPP REVIEW PROJECT PLAN EVALUATION GUIDE
E.   OMB BULLETIN 89-17
F.   ABBREVIATIONS AND ACRONYMS
G.   APPLICABLE LAWS AND REGULATIONS AS REPORTED BY CSPPs
H.   APPLICABLE GUIDANCE AS REPORTED BY CSPPs
I.   REFERENCES
J.   EXAMPLES OF AGENCY REACTIONS TO CSPP REVIEWS

APPENDIX A

THE COMPUTER SECURITY ACT OF 1987

COMPUTER SECURITY ACT OF
1987

Public Law 100-235
100th Congress

An Act

To provide for a computer standards program within the National Bureau of Standards, to provide for Government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Security Act of 1987".

SEC. 2. PURPOSE.

(a) IN GENERAL.—The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

(b) SPECIFIC PURPOSES.—The purposes of this Act are—

(1) by amending the Act of March 3, 1901, to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate;

(2) to provide for promulgation of such standards and guidelines by amending section 111(d) of the Federal Property and Administrative Services Act of 1949;

(3) to require establishment of security plans by all operators of Federal computer systems that contain sensitive information; and

(4) to require mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

SEC. 3. ESTABLISHMENT OF COMPUTER STANDARDS PROGRAM.

The Act of March 3, 1901 (15 U.S.C. 271-278h), is amended—

(1) in section 2(f), by striking out "and" at the end of paragraph (18), by striking out the period at the end of paragraph (19) and inserting in lieu thereof: "; and", and by inserting after such paragraph the following:

"(20) the study of computer systems (as that term is defined in section 20(d) of this Act) and their use to control machinery and processes.";

(2) by redesignating section 20 as section 22, and by inserting after section 19 the following new sections:

"SEC. 20. (a) The National Bureau of Standards shall—

"(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

"(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code;

"(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

"(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code; and

"(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

"(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

"(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

"(b) In fulfilling subsection (a) of this section, the National Bureau of Standards is authorized—

"(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

"(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(3) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(4) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987;   Regulations.

"(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to

.devise techniques for the cost-effective security and privacy of sensitive information in Federal computer systems; and

"(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

"(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

"(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a) (3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

"(c) For the purposes of—

"(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a)(1) and (a)(3), and

"(2) performing research and conducting studies under subsection (b)(5),

the National Bureau of Standards shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the National Bureau of Standards determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

"(d) As used in this section—

"(1) the term 'computer system'—

"(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

"(B) includes—

"(i) computers;

"(ii) ancillary equipment;

"(iii) software, firmware, and similar procedures;

"(iv) services, including support services; and

"(v) related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949;

"(2) the term 'Federal computer system'—

"(A) means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function; and

"(B) includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949;

"(3) the term 'operator of a Federal computer system' means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer

system on behalf of the Federal Government to accomplish a Federal function;

"(4) the term 'sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

"(5) the term 'Federal agency' has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.

15 USC 278g-4.

"Sec. 21. (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

"(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industries;

"(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

"(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

"(b) The duties of the Board shall be—

"(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

"(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

"(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress.

Reports.

"(c) The term of office of each member of the Board shall be four years, except that—

"(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

"(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

"(d) The Board shall not act in the absence of a quorum, which shall consist of seven members.

"(e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board

Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

"(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.

"(g) As used in this section, the terms 'computer system' and 'Federal computer system' have the meanings given in section 20(d) of this Act."; and

(3) by adding at the end thereof the following new section:

National Bureau of Standards Act. 15 USC 271 note.

"SEC. 23. This Act may be cited as the National Bureau of Standards Act.".

SEC. 4. AMENDMENT TO BROOKS ACT.

Section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(d)) is amended to read as follows:

"(d)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 20(a) (2) and (3) of the National Bureau of Standards Act, promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of

President of U.S.

Federal Register, publication.

Federal computer systems. The President may disapprove or modify such standards and guidelines if he determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be submitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

"(2) The head of a Federal agency may employ standards for the cost-effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

"(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by Government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effective implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United States

Federal Register, publication.

Code. Notice of each such waiver and delegation shall be transmitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental

Affairs of the Senate and shall be published promptly in the Federal Register.

"(4) The Administrator shall revise the Federal information resources management regulations (41 CFR ch. 201) to be consistent with the standards and guidelines promulgated by the Secretary of Commerce under this subsection.   Regulations.

"(5) As used in this subsection, the terms 'Federal computer system' and 'operator of a Federal computer system' have the meanings given in section 20(d) of the National Bureau of Standards Act.".

SEC. 5. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.   40 USC 759 note.

(a) IN GENERAL.—Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency. Such training shall be—

(1) provided in accordance with the guidelines developed pursuant to section 20(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section for Federal civilian employees; or

(2) provided by an alternative training program approved by the head of that agency on the basis of a determination that the alternative training program is at least as effective in accomplishing the objectives of such guidelines and regulations.

(b) TRAINING OBJECTIVES.—Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training shall be designed—

(1) to enhance employees' awareness of the threats to and vulnerability of computer systems; and

(2) to encourage the use of improved computer security practices.

(c) REGULATIONS.—Within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided Federal civilian employees under subsection (a) and the manner in which such training is to be carried out.

SEC. 6. ADDITIONAL RESPONSIBILITIES FOR COMPUTER SYSTEMS SECURITY AND PRIVACY.   40 USC 759 note.

(a) IDENTIFICATION OF SYSTEMS THAT CONTAIN SENSITIVE INFORMATION.—Within 6 months after the date of enactment of this Act, each Federal agency shall identify each Federal computer system, and system under development, which is within or under the supervision of that agency and which contains sensitive information.

(b) SECURITY PLAN.—Within one year after the date of enactment of this Act, each such agency shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949, establish a plan for the security and privacy of each Federal computer system identified by that agency pursuant to subsection (a) that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system. Copies of each such plan shall be transmitted to the National Bureau of Standards

and the National Security Agency for advice and comment. A summary of such plan shall be included in the agency's five-year plan required by section 3505 of title 44, United States Code. Such plan shall be subject to disapproval by the Director of the Office of Management and Budget. Such plan shall be revised annually as necessary.

40 USC 759 note.   **SEC. 7. DEFINITIONS.**

As used in this Act, the terms "computer system", "Federal computer system", "operator of a Federal computer system", "sensitive information", and "Federal agency" have the meanings given in section 20(d) of the National Bureau of Standards Act (as added by section 3 of this Act).

40 USC 759 note.   **SEC. 8. RULES OF CONSTRUCTION OF ACT.**

Nothing in this Act, or in any amendment made by this Act, shall be construed—

(1) to constitute authority to withhold information sought pursuant to section 552 of title 5, United States Code; or

Public information.

(2) to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is—

(A) privately-owned information;

(B) disclosable under section 552 of title 5, United States Code, or other law requiring or authorizing the public disclosure of information; or

(C) public domain information.

Approved January 8, 1988.

APPENDIX B

OMB CIRCULAR A-130
MANAGEMENT OF FEDERAL INFORMATION RESOURCES
APPENDIX III
SECURITY OF FEDERAL AUTOMATED INFORMATION SYSTEMS

APPENDIX III
TO OMB CIRCULAR NO. A-130

SECURITY OF FEDERAL AUTOMATED INFORMATION SYSTEMS

1. Purpose

This Appendix establishes a minimum set of controls to be
included in Federal automated information systems security
programs; assigns responsibilities for the security of agency
automated information systems; and clarifies the relationship
between such agency security programs and internal control
systems established in accordance with OMB Circular No. A-123,
Internal Control Systems. The Appendix revises procedures
formerly contained in Transmittal Memorandum No. 1 to OMB
Circular No. A-71, now rescinded, and incorporates
responsibilities from applicable national security directives.

2. Definitions

a. The term "automated information system" means an
information system (defined in Section 6d of the Circular) that
is automated.

b. The term "information technology installation" means
one or more computer or office automation systems including
related telecommunications, peripheral and storage units, central
processing units, and operating and support system software.
Information technology installations may range from information
technology facilities such as large centralized computer centers
to individual stand-alone microprocessors such as personal
computers.

c. The term "sensitive data" means data that require
protection due to the risk and magnitude of loss or harm that
could result from inadvertent or deliberate disclosure,
alteration, or destruction of the data. The term includes data
whose improper use or disclosure could adversely affect the
ability of an agency to accomplish its mission, proprietary data,
records about individuals requiring protection under the Privacy
Act, and data not releasable under the Freedom of Information
Act.

d. The term "sensitive application" means an application
of information technology that requires protection because it
processes sensitive data, or because of the risk and magnitude of
loss or harm that could result from improper operation or
deliberate manipulation of the application.

e. The term "security specifications" means a detailed description of the safeguards required to protect a sensitive application.

3. Automated Information Systems Security Programs

Agencies shall assure an adequate level of security for all agency automated information systems, whether maintained in-house or commercially. Specifically, agencies shall:

- Assure that automated information systems operate effectively and accurately;

- Assure that there are appropriate technical, personnel, administrative, environmental, and telecommunications safeguards in automated information systems; and

- Assure the continuity of operation of automated information systems that support critical agency functions.

Agencies shall implement and maintain an automated information systems security program, including the preparation of policies, standards, and procedures. This program will be consistent with government-wide policies, procedures, and standards issued by the Office of Management and Budget, the Department of Commerce, the Department of Defense, the General Services Administration, and the Office of Personnel Management. Agency programs shall incorporate additional requirements for securing national security information in accordance with appropriate national security directives. Agency programs shall, at a minimum, include four primary elements: applications security, personnel security, information technology installation security, and security awareness and training.

a. Applications Security

(1) Management Control Process and Sensitivity Evaluation. Agencies shall establish a management control process to assure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications, and into significant modifications to existing applications. Management officials who are the primary users of applications should evaluate the sensitivity of new or existing applications being substantially modified. For those applications considered sensitive, the management control process shall, at a minimum, include security specifications and design reviews and systems tests.

(a) Security Specifications. Agencies shall define and approve security requirements and specifications prior to acquiring or starting formal development of the applications. The results of risk analyses performed at the information technology installation where the applications will be processed should be taken into account when defining and approving security

specifications for the applications. Other vulnerabilities of
the applications, such as in telecommunications links, shall also
be considered in defining security requirements. The views and
recommendations of the information technology user organization,
the information technology installation, and the individual
responsible for security at the installation shall be considered
prior to the approval of security specifications for the
applications.

(b) <u>Design Reviews and System Tests</u>. Agencies
shall conduct and approve design reviews and system tests, prior
to placing the application into operation, to assure the proposed
design meets the approved security specifications. The objective
of the system tests should be to verify that required
administrative, technical, and physical safeguards are
operationally adequate. The results of the design reviews and
system tests shall be fully documented and maintained in the
official agency records.

(c) <u>Certification</u>. Upon completion of the system
tests, an agency official shall certify that the system meets all
applicable Federal policies, regulations, and standards, and that
the results of the tests demonstrate that the installed security
safeguards are adequate for the application.

(2) <u>Periodic Review and Recertification</u>. Agencies
shall conduct periodic audits or reviews of sensitive
applications and recertify the adequacy of security safeguards.
Audits or reviews shall evaluate the adequacy of implemented
safeguards, assure they are functioning properly, identify
vulnerabilities that could heighten threats to sensitive data or
valuable resources, and assist with the implementation of new
safeguards where required. They are intended to provide a basis
for recertification of the security of the application.
Recertification shall be fully documented and maintained in the
official agency records. Audits or reviews and recertifications
shall be performed at least every three years. They should be
considered as part of agency vulnerability assessments and
internal control reviews conducted in accordance with OMB
Circular No. A-123. Security or other control weaknesses
identified shall be included in the annual internal control
assurance letter and report required by Circular No. A-123.

(3) <u>Contingency Plans</u>. Agencies shall establish
policies and assign responsibilities to assure that appropriate
contingency plans are developed and maintained by end users of
information technology applications. The intent of such plans is
to assure that users can continue to perform essential functions
in the event their information technology support is interrupted.
Such plans should be consistent with disaster recovery and
continuity of operations plans maintained by the installation at
which the application is processed.

b. Personnel Security. Agencies shall establish and manage personnel security policies and procedures to assure an adequate level of security for Federal automated information systems. Such policies and procedures shall include requirements for screening all individuals participating in the design, development, operation, or maintenance of sensitive applications as well as those having access to sensitive data. The level of screening required by these policies should vary from minimal checks to full background investigations, depending upon the sensitivity of the information to be handled and the risk and magnitude of loss or harm that could be caused by the individual. These policies shall be established for both Federal and contractor personnel. Personnel security policies for Federal employees shall be consistent with policies issued by the Office of Personnel Management.

c. Information Technology Installation Security. Agencies shall assure that an appropriate level of security is maintained at all information technology installations operated by or on behalf of the Federal Government (e.g., government-owned, contractor-operated installations).

(1) Assigning Responsibility. Agencies shall assign responsibility for the security of each installation to a management official knowledgeable in information technology and security matters.

(2) Periodic Risk Analysis. Agencies shall establish and maintain a program for the conduct of periodic risk analyses at each installation to ensure that appropriate, cost effective safeguards are incorporated into existing and new installations. The objective of a risk analysis is to provide a measure of the relative vulnerabilities and threats to an installation so that security resources can be effectively distributed to minimize potential loss. Risk analyses may vary from an informal review of a microcomputer installation to a formal, fully quantified risk analysis of a large scale computer system. The results of these analyses should be documented and taken into consideration by management officials when certifying sensitive applications processed at the installation. Such analyses should also be consulted during the evaluation of general controls over the management of information technology installations conducted in accordance with OMB Circular No. A-123. A risk analysis shall be performed:

(a) Prior to the approval of design specifications for new installations;

(b) Whenever a significant change occurs to the installations (e.g., adding a local area network; changing from batch to online processing; adding dial-up capability). Agency criteria for defining significant change shall be commensurate with the sensitivity of the data processed by the installation.

(c) At periodic intervals established by the agency commensurate with the sensitivity of the data processed, but not to exceed every five years if no risk analysis has been performed during that period.

(3) Disaster and Continuity Plan. Agencies shall maintain disaster recovery and continuity of operations plans for all information technology installations. The objective of these plans should be to provide reasonable continuity of data processing support should events occur that prevent normal operations at the installation. For large installations and installations that support essential agency functions, the plans should be fully documented and operationally tested periodically, at a frequency commensurate with the risk and magnitude of loss or harm that could result from disruption of information technology support.

(4) Acquisition Specifications. Agencies shall assure that appropriate technical, administrative, physical, and personnel security requirements are included in specifications for the acquisition or operation of information technology installations, equipment, software, and related services, whether procured by the agency or by GSA. These security requirements shall be reviewed and approved by the management official responsible for security at the installation making the acquisition.

d. Security Awareness and Training Programs. Agencies shall establish a security awareness and training program to assure that agency and contractor personnel involved in the management, operation, programming, maintenance, or use of information technology are aware of their security responsibilities and know how to fulfill them. Users of information technology systems should be apprised of the vulnerabilities of such systems and trained in techniques to enhance security.

4. Assignment of Responsibilities

a. Department of Commerce. The Secretary of Commerce shall:

(1) Develop and issue standards and guidelines for assuring the security of Federal automated information systems;

(2) Establish standards, approved in accordance with applicable national security directives, for systems used to process sensitive information the loss of which could adversely affect the national security interest; and

(3) Provide technical assistance to Federal agencies in implementing Department of Commerce standards and guidelines.

b. <u>Department of Defense</u>. The Secretary of Defense shall:

(1) Act, in accordance with applicable national security directives, as executive agent of the government for the security of telecommunications and automated information systems that process information the loss of which could adversely affect the national security interest; and

(2) Provide technical material and assistance to Federal agencies concerning security of Federal telecommunications and automated information systems.

c. <u>General Services Administration</u>. The Administrator of General Services shall:

(1) Issue policies and regulations for the physical and environmental security of computer rooms in Federal buildings consistent with standards issued by the Department of Commerce and the Department of Defense.

(2) Assure that agency procurement requests for computers, software, telecommunications services, and related services include security requirements. Delegations of procurement authority to agencies by GSA under mandatory programs, dollar threshold delegations, certification programs, or other so-called blanket delegations shall include requirements for agency specification of security requirements.

(3) Assure that information technology equipment, software, computer room construction, guard or custodial services, telecommunications services, and any other related services procured by GSA meet the security requirements established and specified by the user agency and are consistent with other applicable policies and standards issued by OMB, the Department of Commerce, the Department of Defense, and the Office of Personnel Management.

(4) Issue appropriate standards for the security of Federal telecommunications systems. Standards related to systems used to communicate sensitive information, the loss of which could adversely affect the national security interest, shall be developed and issued in accordance with applicable national security directives.

d. <u>Office of Personnel Management</u>. The Director, Office of Personnel Management, shall maintain personnel security policies for Federal personnel associated with the design, programming, operation, maintenance, or use of Federal automated information systems. Requirements for personnel checks imposed by these policies should vary commensurate with the risk and magnitude of loss or harm that could be caused by the individual. The checks may range from merely normal reemployment screening procedures to full background investigations.

5. Reports

In their annual internal control report to the President and the Congress, required under OMB Circular No. A-123, agencies shall:

    a.   Describe any security or other control weaknesses identified during audits or reviews of sensitive applications or when conducting risk analyses of installations; and

    b.   Provide assurance that there is adequate security of agency automated information systems.

APPENDIX C

OMB BULLETIN 88-16
GUIDANCE FOR PREPARATION AND SUBMISSION OF SECURITY PLANS FOR
FEDERAL COMPUTER SYSTEMS CONTAINING SENSITIVE INFORMATION

OMB BULLETIN NO. 88-16

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

SUBJECT: Guidance for Preparation and Submission of Security
          Plans for Federal Computer Systems Containing
          Sensitive Information

1. <u>Purpose</u>. The purpose of this Bulletin is to provide guidance
to agencies on preparing and submitting computer security plans
required by the Computer Security Act of 1987.

2. <u>Authority</u>. The Computer Security Act of 1987 (P.L. 100-235),
referred to in this Bulletin as "the Act," requires Federal
agencies to identify each computer system which contains
sensitive information and to prepare a plan for the security and
privacy of each such system. The Act further requires that
agencies submit their security plans to NBS and NSA for advice
and comment and makes such plans subject to OMB disapproval.

3. <u>Definitions</u>. See Appendix A.

4. <u>Objectives of Security Plan Review Process</u>. The security
plan review process is designed to reduce the risk and magnitude
of harm that could result from the loss, misuse or unauthorized
access to or modification of information in Federal computer
systems.   It is intended to help agencies identify and assess:

    o the nature and extent of sensitive information systems
       in government agencies and the security requirements of
       such systems;

    o the adequacy of security planning and basic
       administrative and technical approaches used in
       protecting sensitive systems;

    o the requirements for additional guidance, standards,
       assistance, training, and new technology to improve
       protection of sensitive and valuable information
       resources.

5. <u>Applicability</u>. This Bulletin applies to Federal agencies
as defined in Section 3(b) of the Federal Property and
Administrative Services Act of 1949, as amended.

a. <u>Contractor and Other Systems</u> - The Act requires that agencies identify and prepare security plans for all Federal computer systems which contain sensitive information. This includes systems that process sensitive information operated by a contractor or other organization on behalf of the Federal Government to accomplish a Federal function. Plans for these systems must be included in the agency's submission; they are not to be submitted separately by the contractor or other organization.

b. <u>Classified Systems</u> - The provisions of the Act and this guidance do not apply to systems containing classified information, systems involving intelligence activities, cryptologic activities related to national security, direct command and control of military forces, equipment that is integral to a weapons system or direct fulfill- ment of military or intelligence missions (excluded by 10 U.S.C. 2315), or mixed classified/unclassified systems, provided such systems are always operated under rules for protecting classified information.

6. <u>Action Required</u>. In accordance with the Act, each agency must:

o By July 8, 1988 - identify systems under its supervision which contain sensitive information, and

o By January 8, 1989 - prepare security plans for each identified system and submit them to NBS and NSA for advice and comment.

Guidance for identifying systems and preparing security plans is provided below and in Appendix B.

7. <u>Identification of Systems Containing Sensitive Information</u>. It is the responsibility of each agency to identify systems which contain sensitive information by applying the definition of "sensitive information" (See Appendix A) in the context of its own mission.

a. <u>Identifying and Delineating Systems</u>. The key to the security plan submission process lies in the identification and delineation of systems which contain sensitive information. Agencies must draw the logical boundaries around such systems for planning and reporting purposes.

Separate submissions do not have to be prepared for systems which have essentially the same function, characteristics, security needs, and security plans. Agencies may, for the purpose of these submissions, treat two or more systems as a single system. Agencies

will be required to indicate in their security plans which systems are actually a group of systems treated as one.

It is not intended that agencies report separately on every minicomputer or small computer system (or even every mainframe). However, it should also be clear that treating all of an entire agency's systems as a single generic group would, except for a small agency with homogeneous systems, be inconsistent with the objectives of this Bulletin.

b. Categories of Systems. For the purpose of reporting, systems should be grouped into two basic categories: 1) major application systems and 2) general ADP support systems as described below.

Major application systems are systems that perform clearly defined functions and for which there are clearly identifiable security considerations and needs. Such a system might comprise many individual application programs and hardware, software, and telecommunications components at more than one site. Examples might include a major agency benefits payment system, or a group of systems all supporting a specific agency program.

General ADP support systems consist of hardware and software that provide general ADP support for a variety of users and applications. Individual application systems are less easily distinguished than in the previous category but such applications may contain sensitive data. Even if none of the individual applications are sensitive, the support system itself could be considered sensitive if it provides critical support for the mission of the agency.

Several types of systems may be covered by this category. Examples include:

o   an agency computer center, facility, or site
o   an agency-wide data network
o   a local area network
o   a grouping of personal computer workstations, perhaps connected by a local area network.

8. Format and Content of Security Plans. In accordance with the Act, agencies are required to prepare and submit a plan for each identified system. Each system plan must include a basic description of the purpose, environment, and sensitivity of the system and the security measures intended to protect the system and its data. These plans are not to be simply statements of agency security policy. They should indicate security requirements and how the agency intends to meet those requirements.

In addition to the individual plans, an agency, at its option, may include a brief overview of its security and privacy program which identifies agency-wide security measures or concerns.

Agencies are requested to prepare their system plans in accordance with the structure and format described in Appendix B.

9. Submission of Materials.

    a. Submission Date. In accordance with the Act, agency submissions should be received by January 8, 1989.

    b. Submission Address. Agency submissions should be sent to the following address.

        > Computer Security Plan Review Team
        > National Bureau of Standards
        > Technology Building
        > Gaithersburg, MD 20899

    c. Handling of Submissions. Submissions will be jointly reviewed by NBS and NSA staff, and advice and comment will be transmitted directly back to the submitting agency. All submitted materials will be treated as For Official Use Only (FOUO) information.

    d. Automated Submissions. Agencies wishing to submit their plans by automated media should contact Dennis D. Steinauer for more information.

10. Information Contacts. Questions regarding format or submission should be directed to Dennis D. Steinauer, telephone: (301) 975-3357. Other questions regarding this Bulletin should be directed to Edward C. Springer, telephone: (202) 395-4814.

James C. Wyle III
Director

Attachments

DEFINITIONS

For the purposes of this guidance, the following definitions from the Act apply.

"'Computer System' means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and includes:

- o computers;
- o ancillary equipment;
- o software, firmware, and similar procedures;
- o services, including support services; and
- o related resources as defined by regulations issued by the Administrator of General Services pursuant to section 111 of the Federal Property and Administrative Service Act of 1949."

"'Federal Computer System' means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal government to accomplish a Federal function and includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949."

"'Sensitive Information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

In addition, the following definition from the Federal Property and Administrative Services Act of 1949, as amended, applies.

"The term 'Federal agency' means any executive agency or any establishment in the legislative or judicial branch of the government (except the Senate, the House of Representatives, and the Architect of the Capitol and any activities under his direction)." (40 U.S.C. 472)

INSTRUCTIONS FOR PREPARING SYSTEM SECURITY PLANS

GENERAL

The purpose of the agency system security plan is to provide a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. It is not intended to be a detailed technical description of system content, risks, or security mechanisms. Each security plan should have four sections:

- o Basic System Identification
- o Sensitivity of Information
- o System Security Measures
- o Needs and Additional Comments

As indicated in the main body of this guidance, an agency may submit an overview of its overall security program. This overview is optional and is not a substitute for individual security plans. The format and content of the agency's overview, if provided, is left to the discretion of the submitting agency. However, the overview should not exceed five pages in length.

This appendix contains a description of the intended scope, content, and format of each section of individual system security plans.

1. BASIC SYSTEM IDENTIFICATION

This section of the plan contains basic identifying information about the system. It should include the following information.

Reporting Department or Agency

Organizational Subcomponent - Bureau or subagency

Operating Organization - The name of the organization responsible for direct operation or supervision of the system, if different from above. For example, this might be a contractor.

System Name/Title

System Category - One of the following:

- o Major application
- o General ADP support system

Level of Aggregation - One of the following:

o   Single identifiable system.

o   Group of similar systems having
    sufficiently similar characteristics and
    security requirements as to be managed and
    reportable as a single system.

Operational Status - One of the following:

o   Operational - system is currently in
    operation.

o   Under Development - system is currently
    under design, development, or implementation.

General Description/Purpose - A brief (1-2 paragraph)
description of the function and purpose of the system.

System Environment and Special Considerations - A brief
general description of the physical, operational, and
technical environment in which the system operates.   The
location, types of computer hardware and software involved,
types of users served, or other special considerations should
be described.   For example, if an application makes
substantial use of a data processing facility outside the
direct control of the agency, this should be indicated.
Similarly, if a general ADP support system (e.g., a data
center) serves a substantial external (non-agency) customer
base, this should also be indicated.

Information Contact(s) - The name and telephone number of one
or more persons designated to be the point of contact for
this system.   The designated persons should have sufficient
knowledge of the system to be able to provide the review team
with additional information or points of contact, as needed.

2.   SENSITIVITY OF INFORMATION HANDLED

This section should provide a description of the types of
information handled by the system and should provide the basis
for the system's security requirements.   It should contain the
following information:

General Description of Information Sensitivity - Describe, in
general terms, of the nature of the information handled by
the system and the need for protective measures.

Applicable Laws or Regulations Affecting the System - List
any laws or regulations that establish specific requirements
for confidentiality of information in the system. Examples
might include the Privacy Act or a specific statute or
regulation affecting information the agency processes (e.g.,
tax or census data). Note: This should not be a list of
technical standards (e.g., FIPS 46) which determine how
certain types of security mechanisms are to be implemented
once the need for such protection has been determined. For
similar reasons, the Computer Security Act of 1987 should not
be listed.

System Protection Requirements - A system may need protection
for one or more of the following reasons:

   o Confidentiality - The system contains information that
      requires protection from unauthorized disclosure.
      Examples: For Official Use Only, timed or controlled
      dissemination (e.g., crop report data), personal data
      (covered by Privacy Act), confidential (proprietary)
      business information.

   o Integrity - The system contains information which must
      be protected from unauthorized modification. Examples:
      Funds transfer systems.

   o Availability - The system contains information or
      provides services which must be available on a timely
      basis to meet mission requirements or to avoid other
      types of losses (e.g., financial). Example: Operational
      control or monitoring systems.

A given system may contain several types of information, thus
affecting the relative importance of each type of protection
for that system. The purpose of this section is to indicate
the type and relative importance of protection needed for the
identified system.

For each of the three categories listed above (Confidentiality,
Integrity, Availability), indicate if the protection
requirement is:

   o Primary (i.e., a primary security concern of the
      system),
   o Secondary, or
   o Minimal concern or not applicable

"Primary" may be indicated for more than one of the categories,
if appropriate.

3. SYSTEM SECURITY MEASURES

This section should describe the measures (in place or planned) that are intended to meet the protection requirements of the system. The types of protective measures should be consistent with the requirements described in the previous section.

Risk Assessment - How were the risks and associated protection requirements for this system determined? Indicate whether by:

  o Formal risk analysis, or
  o Other means (Please describe)

Applicable Guidance - Indicate, to the extent practical, specific standards or other guidance used in the design, implementation, or operation of the protective measures used on the system (e.g., relevant Federal or industry standards).

Security Measure Status - Basic categories of protective measures are outlined below. For each category of protective measure, there should be an indication of the applicability and status of that category of control measure in the identified system.

  o In Place - Control measures of the type described are in
    place and operational, and judged to be effective. Do
    not decribe the details of the specific control
    measures.

  o Planned - Specific control measures (new, enhanced,
    etc.) are planned for the system. A general description
    of the planned measures and expected operational dates
    should be provided.

  o In Place and Planned - Some measures are in place, while
    others are planned. A general description of the
    planned measures and expected operational dates should
    be provided.

  o Not applicable - This type of control measure is not
    needed or appropriate for this system.

It should be noted that for an operational system, some specific controls of a given type may be "In Place" while others may be "Planned". For a system under development, it is expected that most measures will be "Planned". For each area in which controls are planned rather than operational, there should be a brief description of the measures planned for the system and the expected operational date(s).

Security Measures

Following are two lists of basic categories of control: one for major application systems and one for general ADP support systems. Use the list of categories that corresponds to the type of system this plan describes.

SECURITY MEASURES - MAJOR APPLICATION SYSTEMS

The following categories of security controls should be addressed for systems which have been identified as Major application systems.

MANAGEMENT CONTROLS - overall management controls of the application system.

Assignment of Security Responsibility
Risk/Sensitivity Assessment
Personnel Selection/Screening

DEVELOPMENT CONTROLS - procedures to build protection into the application system during system development.

Security Specifications
Design Review and Testing
Certification/Accreditation

OPERATIONAL CONTROLS - day-to-day procedures and mechanisms to protect operational application systems.

Production, I/O Controls
Contingency Planning
Audit and Variance Detection
Software Maintenance Controls
Documentation

SECURITY AWARENESS AND TRAINING - security awareness and training of users and technical staff concerning the application system.

Security Awareness and Training Measures

TECHNICAL CONTROLS - hardware and software controls to provide automated protections.

User Identification and Authentication
Authorization/Access Controls
Data Integrity/Validation Controls
Audit Trails and Journaling

SUPPORT SYSTEM SECURITY MEASURES - adequate security measures are provided by the facility(ies), network, etc. where the application system is processed.

Security Measures for Support System(s)

SECURITY MEASURES - GENERAL ADP SUPPORT SYSTEMS

The following categories of security controls should be addressed for systems which have been identified as General ADP Support Systems.

MANAGEMENT CONTROLS - overall management controls of the support system.

Assignment of Security Responsibility
Risk Analysis/Assessment
Personnel Selection/Screening

DEVELOPMENT/INSTALLATION - procedures to build protection into the computer system.

Acquisition Specifications
Certification/Accreditation

OPERATIONAL CONTROLS - day-to-day procedures and mechanisms to protect operational systems.

Physical and Environmental Protection
Production, I/O Controls
Emergency, Backup and Contingency Plans
Audit and Variance Detection
System Software Controls
Documentation

SECURITY AWARENESS AND TRAINING - security awareness and training of technical staff and users of the system.

Security Awareness and Training Measures

TECHNICAL CONTROLS - hardware and software controls in the system to provide automated protections.

User Identification and Authentication
Authorization/Access Controls
Audit Trail Mechanisms
Confidentiality Controls (e.g., encryption)
Integrity Controls (e.g., message authentication)

APPLICATION SYSTEM CONTROLS - adequate security measures are in application systems which operate on the subject general purpose system.

Security measures for application systems.

4. NEEDS AND ADDITIONAL COMMENTS

This final section is intended to provide an opportunity to include additional comments about the security of the subject system. Of particular value will be identification of the needs for specific guidance, standards, or other tools to improve protection for the subject system.

APPENDIX D

CSPP REVIEW PROJECT PLAN EVALUATION GUIDE

Computer Security Plan Review Project

Computer Security & Privacy Plan

Plan Evaluation Guide

Table of Contents

- i -

I.   INTRODUCTION

This guide is provided for use during the review and analysis of computer security and privacy plans (CSPPs) required to be submitted pursuant to Public Law (P.L.) 100-235, The Computer Security Act of 1987 (CSA).   The CSA requires that Federal agencies identify each computer system which processes, stores, or transmits sensitive information.   The CSA further requires that agencies prepare a CSPP for each such system. These plans are to be submitted to the National Institute for Standards and Technology (NIST, formerly National Bureau of Standards) and the National Security Agency (NSA) for advice and comment.   On July 6, 1988, the Office of Management and Budget (OMB) issued Bulletin Number 88-16 (OMB 88-16), providing guidance to the heads of executive departments and agencies in the preparation and submission of the CSPPs.   It should be noted that Congressional and Independent agencies have NOT been exempted from the CSA requirements.   These organizations are also required to comply with the submission requirements as outlined in OMB 88-16.

In order to limit the level of effort required to efficiently review each plan submitted, and to ensure a cost effective and consistent approach to the review and comment process, NIST and NSA have agreed to establish a single review process, jointly staffed and managed by NIST and NSA staff.   Staff selected by the two reviewing agencies are to play a key role in completing the first cycle of review and comment in implementing this landmark legislation.   These key staff have been organized into review teams.   Teams will be assigned responsibility for reviewing and providing comments and recommendations on the submissions received from covered agencies.

This Analysis Guide (Guide) is provided for use by review team leaders and team members in evaluating agency computer security program summaries and sensitive system plans.   As with any guide, it is not intended to provide a fixed, prescriptive framework for assessing and responding to agency submissions.   Rather, it should be viewed as a road map to be used by team leaders and reviewers, providing focus for the review process.

Team leaders and members have a wide range of experiences and skills in data processing and computer security.   All project members are expected to draw upon each other's expertise in completing their analyses.

Both NIST and NSA view this first review activity as critical to the success of the CSA in increasing the protections afforded to sensitive Federal information.   All members of the review staff are expected to apply the highest standards of personal and professional competence to the completion of this crucial task.

II. ROLES AND RESPONSIBILITIES

Each member of the CSPP Review Project team has a key role to play in the successful completion of the Project. This chapter provides a brief description of the roles and responsibilities of Project participants in order that they may better understand the Project structure as well as their specific responsibilities in making it a success.

General Responsibilities

For the duration of their assignment to the Project, all U. S. Government personnel are expected to adhere to accepted standards of conduct for federal employees.

Working Relationships - The CSPP Review Project is organized (informally) as shown in Figure 1 on the following page. The Project staff is made up of management, administrative, clerical, technical, and professional personnel from NIST and NSA. These individuals bring a variety of backgrounds, knowledge, training, and experience to the Project.

Successful completion of what can only be described as a monumental task, within the prescribed time frames, will require that all Project staff be prepared to bring an extra measure of courtesy, respect, and consideration to their tasks. The Project managers expect that all interactions will remain on a professional, business level, with each of us maintaining our focus on the primary objective of the Project:

> assisting Federal agencies in improving the security of sensitive Federal information which is stored, processed, or transmitted using computer resources.

Confidentiality of Information - By submitting their CSPPs to the Project, agencies have entrusted us with information which may be extremely sensitive. All CSPPs must be treated as sensitive to disclosure by all Project staff.

All CSPPs submitted for review will be logged, assigned a tracking number, and the assigned location for each plan will be tracked throughout the review process. Materials should be kept in locked or protected areas when they are not being specifically worked on and must be secured before you depart from the project site at the close of business each day.

Project staff and support contractors are not to discuss the content of CSPPs, analyses, or opinions regarding submitted materials or analyses with any individual not currently assigned to and working on the Project. All information to be disseminated outside of the Project with regard to the CSPPs, including analyses, reports, summaries, analyses, etc. should be specifically channelled through the Project Managers. Extra care should also be taken not to discuss any classified computer security information in either agency analyses or conversation with project staff.

COMPUTER SECURITY & PRIVACY PLAN REVIEW PROJECT

```
┌─────────────────────┐              ┌─────────────────────┐
│ NATIONAL INSTITUTE OF│              │      NATIONAL        │
│   STANDARDS AND      │              │      SECURITY        │
│     TECHNOLOGY       │              │       AGENCY         │
└──────────┬──────────┘              └──────────┬──────────┘
           │                                    │
           ▼                                    ▼
┌─────────────────────┐              ┌─────────────────────┐
│       NIST          │──────────────│       NSA            │
│   Project Manager   │              │   Project Manager    │
└─────────────────────┘              └─────────────────────┘

     ┌─────────────────┐
     │   Preliminary   │
     │     Review      │
     │      Team       │
     └─────────────────┘                ┌─────────────────┐
                                         │   Contractor    │
     ┌─────────────────┐                 │     Staff       │
     │  Administrative │                 └─────────────────┘
     │   & Clerical    │
     │      Staff      │
     └─────────────────┘

┌─────────────────┐                         ┌─────────────────┐
│  Team Leader    │                         │  Team Leader    │
│  Review Team    │    ●      ●      ●       │  Review Team    │
│     # 1         │                         │      #6         │
└─────────────────┘                         └─────────────────┘
```
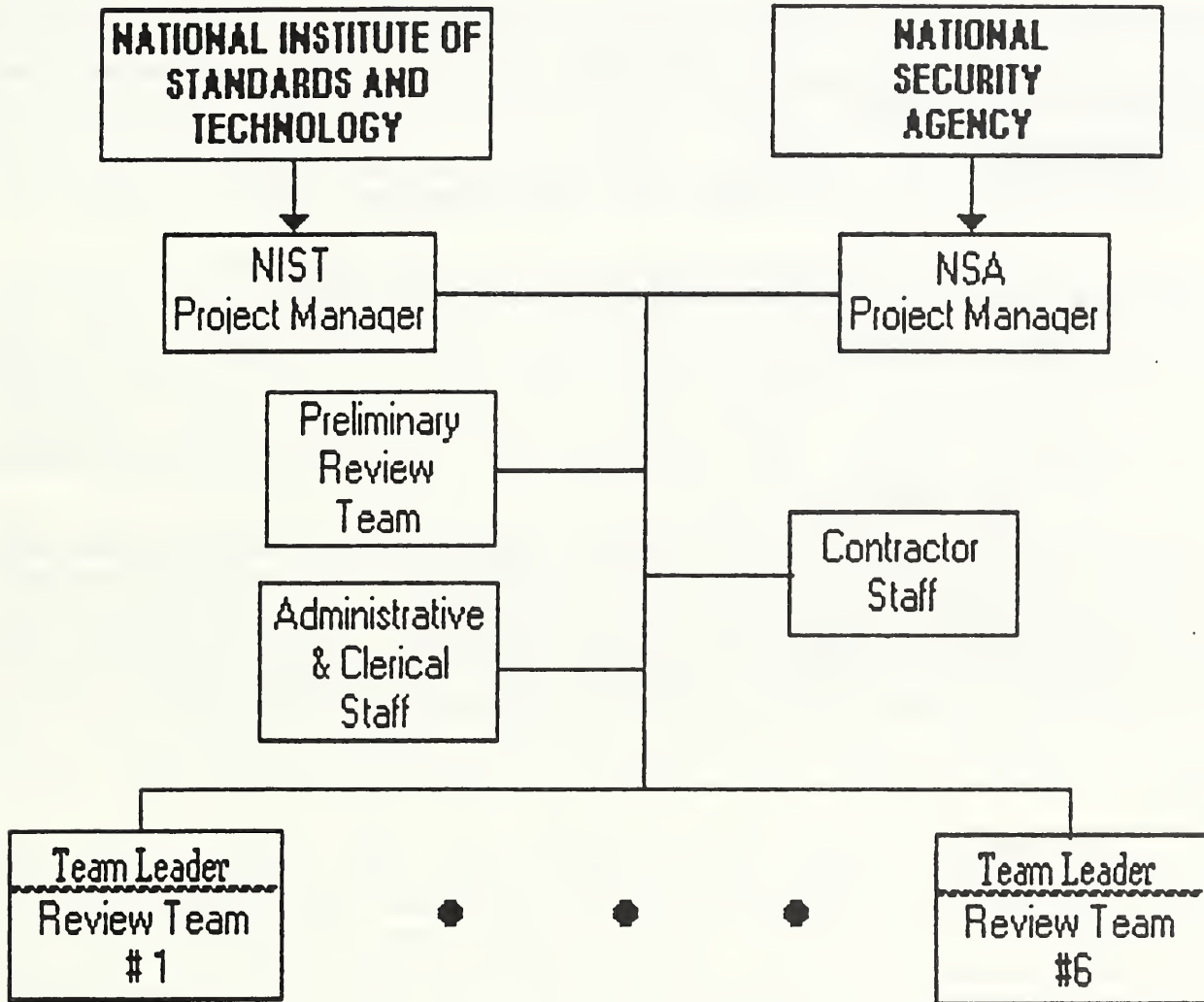
Figure 1 - Project Organization

Contractor Support - Because we will be working closely, on a day-to-day basis with contractor staff and will be housed in contractor provided space, it is appropriate to remind all Project staff that contractor personnel perform work against a task order, and that all changes, modifications, etc. to that work must be made by the task managers. For the CSPP Review Project, the task managers are the Project Managers from NIST and NSA, Mr. Douglas Hunt and Mr. Christopher Bythewood, respectively.

Team Members

Professional and technical staff assigned as review team members have two primary responsibilities:

1. Completing the review and analysis of agency Computer Security and Privacy Plans (CSPPs); and

2. Preparing comments and recommendations to submitting agencies based upon their analysis of each CSPP.

Because of the nature of tasks facing the Project team, activities which are primarily administrative or clerical in nature may, from time-to-time, be assigned to professional and technical staff. Project staff are expected to accept and carry out all assignments in the most professional and responsible manner possible.

All team members are expected to extend their full cooperation and support to their designated Team Leader, accepting and completing all assigned review activities in a professional manner. Additionally, team members are expected to provide assistance, support, and cooperation to their professional and technical colleagues in the completion of their assigned review, data extraction, and tracking responsibilities.

Team Leaders

The Project Managers will designate a Leader for each review team. In addition to their CSPP review responsibilities, Team Leaders will be expected to organize and coordinate the assignment and completion of review activities for their team. Team Leaders are expected to provide guidance to team members in the review and evaluation process, as well as ensure that the highest professional standards are maintained, while making every effort to meet established time constraints.

Team Leaders will have the additional responsibility of reviewing agency computer security program overviews and summaries, and for reviewing the analyses and recommendations of their team members regarding each CSPP, to ensure that they are consistent with this guide. Team leaders will also be expected to prepare an Agency Analysis Summary based upon their review of the agency program summary and the analyses and recommendations of their team for each CSPP.

III. DATA COLLECTION

COMPLETE DATA COLLECTION INSTRUCTIONS TO BE PROVIDED UPON COMPLETION OF DATA BASE DESIGN AND PROGRAMMING

Initial Logging Procedures

Each separate document contained in the submission will be stamped with a unique sequence number and the beginning and ending sequence numbers will be entered into the document log. Upon receipt at the Glenwood site, submissions will be assigned for logging into the plan tracking system by submitting agency. In order to ensure that all submissions from an agency are properly logged, the same personal computer system will be used to log all documents received from a given agency.

Data collected during initial entry into the tracking system include the document sequence number, the reporting department or agency; agency acronym; the responsible organizational subcomponent; the operating organization and an indication if this is a contractor; and the system name/title.

Keyword Instructions

Keywords are to be selected from the listing of words provided by the data capture program or in Appendix F to this guide. Keywords capturing the primary elements and concepts of the item should be entered in the space provided on the CSPP data capture sheet or directly into the CSPP database, as appropriate. If the reviewer identifies a more appropriate and/or additional keyword(s) for an item, he/she should note the new keyword(s) on the data capture forms or in the area provided in the automated data entry program, and bring it to the attention of their team leader for addition to the listings and the capture program.

IV. PRELIMINARY REVIEW

As CSPPs are received by the project they will be logged and each document will be automatically assigned a tracking number. At the completion of logging activities the agency submission will be forwarded for preliminary review. During this process, project staff will review the CSPPs included in the agency submission to ensure that they are complete enough to be forwarded for complete review and analysis. At the same time, staff conducting the preliminary review will capture a significant portion of the CSPP data items not requiring keyword identification.

To be adequate for review team action the submission may not consist of a single plan covering all agency systems, except in the case of small and micro agencies (those having a few hundred employees or less). Additionally, CSPPs must, at a minimum, contain:

1. A system description that identifies at least "generic" types of information (e.g.: payroll, personnel, administrative) and at least "generic" types of processing to be accomplished (e.g.: financial management, decision support).

2. A description of the reasons the system has been identified as sensitive, and an indication that at least one of the indicated sensitivity reasons (confidentiality, integrity, and availability) is a primary concern.

3. At least some controls identified as "in place" or "planned".

Plans not meeting the above criteria should be separated from the agency submission and forwarded to the Project Managers.

V. AGENCY PROGRAM OVERVIEW ANALYSIS

In addition to requiring the submission of CSPPs for systems processing sensitive information, OMB Bulletin 88-16 provides agencies the option of including a "brief overview of its security and privacy program which identifies agencywide security measures or concerns." It is anticipated that agencies, particularly larger agencies, will elect to provide a program overview.

While no specific format or content has been prescribed for the program overview, it is anticipated that the overview documents submitted will typically address the following major topics:

-- agencywide computer security policies, procedures, standards, and requirements;

-- the agencywide computer security and privacy program structure and operations;

-- agencywide computer security and privacy controls and protections which may not be adequately reflected in the individual plans; and

-- agency level concerns with the CSPP process and requirements and agency level needs for guidance, standards, and technology.

Agency CSPPs should be developed within the context of an agencywide computer security program. Without clear agency policy, procedures, standards, and requirements for computer security it is likely that individual CSPPs may not be comprehensive. The Overview sets the context within which each of the CSPPs from an agency must be analyzed.

Team leaders (see chapter II) are expected to complete the review of agency Overview submissions. In addition to providing their comments and recommendations with regard to the agency security policy and program, this will provide the team leader with a more complete context for the preparation of the final agency summary (see Chapter VI).

Specific areas for attention during the review of the agency program summary are:

Agencywide Policy or Directive

The essential elements of an effective and complete agencywide computer security policy or directive are:

-- a specific statement of an agency position on the protection of automated information and processing resources;

-- assignment of specific responsibilities for computer and automated information to agency senior management officials;

--   establishment of a single focus for the agencywide implementa-
      tion, coordination, and monitoring of the policy or
      directive; and

--   establishment of broad, general requirements for implementing
      the policy or directive.

The reviewer should attempt to determine if there is an agencywide
computer security policy or directive, and if so, whether a copy is
included in the agency program summary. If a copy of the policy or
directive has not been included the reviewer should note this and
briefly iterate the elements listed above in the final agency
summary and recommendations. In the event that the policy has been
provided but significant deficiencies are identified, recommenda-
tions for improvement should be included.

       While we should not attempt to instruct agencies as to
       what their specific policies should be, who should carry
       them out, or what should be required, it is important
       that all of the essential elements be present and provide
       a reasonable basis on which to implement an agency
       computer security program.

Computer Security Program Structure

In order to be most effective, an agencywide computer security
program should be structured so as to provide:

--   high visibility and access to the agency's most senior
      management for computer security program management;

--   direct policy and management relationships between senior
      computer security program managers and policy makers, and
      computer security program officials throughout the agency;

--   oversight and accountability for the implementation of
      computer security requirements and standards at the system
      level; and

--   a formal management and reporting structure which provides
      for formal periodic reporting to senior agency management.

The reviewer should attempt to identify the overall agency program
structure and the extent to which the above elements can be
achieved through that structure. Lines of authority and
responsibility should be clear and unencumbered by potential
conflicts of interest, particularly at the senior and
suborganizational program management levels. Such conflicts are
most likely to occur if computer security management personnel are
located within computer support or operations organizations, or
even within the physical security office.

The review process should not attempt to direct a particular agency organizational alignment. It should be used, however, to identify the possible blurring of lines of authority, responsibility, and accountability which could result in a less effective agencywide program.

If the reviewer identifies potential weaknesses in the structure presented in the program summary, these should be identified in both the comments to the program overview and in the final summary analysis. In the event that the reviewer cannot determine the agency's computer security program structure from the materials provided, this should be noted in the program overview analysis and the agency should be reminded of the important elements of such a program in the final agency analysis.

Agencywide Controls and Protections

An agencywide computer security program may well provide certain baseline protections and controls for the entire agency. (This will be particularly true in small to medium sized agencies with a limited number of systems and processing locations.) If, during the review of the agency program overview, it is determined that such controls and protections have been provided on an agencywide basis, the Team Leader should note these items and immediately apprise his/her team members of these items.

In addition to the standard review items identified in Chapter 5 for consideration in relation to all identified controls and protections, the following issues should be considered in relation to agencywide controls and protections:

1.   The responsibility for implementing agencywide controls should be clearly established; and

2.   A mechanism or procedure for monitoring the implementation and effectiveness of agencywide controls should be established.

The reviewer should include the results of her/his analysis of and recommendations regarding agencywide controls and protections in the comments analysis of the agency program overview. Where possible significant deficiencies are identified in the agencywide controls or their implementation, these should also be included in the final agency summary.

Agency Level Concerns

Agencies may have global concerns over the CSPP process, or needs for guidance, standards, and computer security related technology. The reviewer should include any such comments in their sheet and ensure that they are highlighted for the Project Managers' attention.

VI. Plan Analysis Guide

The review and analysis of individual CSPPs is the heart of the entire review process. As indicated in OMB Bulletin 88-16, the three primary objectives of the plan review process are to identify and assess the extent to which agencies have

> -- identified the nature and extent of their sensitive information and systems and assessed the security requirements for those systems, and

> -- initiated security planning and implemented basic technical and administrative approaches to protect their sensitive systems;

and to assist the Computer Security Advisory Board, NIST, and NSA in

> -- identifying requirements for additional guidance, standards, training, new technology, or other assistance to improve the protection of sensitive and valuable information resources.

As described in OMB Bulletin 88-16, the CSPPs are not intended to provide a detailed statement of security protections in place for any system. Rather, the CSA established the CSPP preparation requirements to provide a framework within which agencies can assess their computer security needs, and identify and implement cost effective protections which meet those needs. The reports required by OMB Bulletin 88-16 are intended to provide "a basic overview of the security and privacy requirements of the [identified] system[s] and the agency's plan for meeting those requirements."

As indicated in Chapter IV of this guide, Preliminary Review, prior to assignment to a review team, all CSPPs receive a preliminary review top ensure that at least a minimum amount of information is included. At the same time, as much information as possible will have been captured on a preliminary review data sheet or entered directly into the plan review database. Some of the following review areas include instructions for capturing similar information. It is not necessary to recapture or records information already recorded during the preliminary review. In some cases, however, the preliminary reviewer could not readily identify some items, these will be left blank. The reviewer should attempt to discover this information during his/her analysis of the plan.

If a reviewer receives a plan which is not accompanied by a preliminary review data sheet they should notify their team leader who will request that a copy be printed.

All CSPPs are to contain four basic parts:

1. <u>Basic System Identification</u> - This part contains the information necessary to identify the basic system characteristics and its operating environment.

2. <u>Sensitivity of Information Handled</u> - This should provide a report of the nature of the sensitivities and an overview of the protection requirements.

3. <u>System Security Measures</u> - This part should reflect the methods used to determine the specific protection requirements and should identify the control areas in which protections have been implemented or are planned to be implemented.

4. <u>Needs and Additional Comments</u> - Agencies may provide additional comments relative to the security needs and protections for the system, as well as an indication of requirements for additional guidance, standards, technology, training, or other assistance.

In completing their analysis of agency CSPPs reviewers are expected to reach broad, general conclusions and make generalized recommendations with respect to the control areas and general types of protections which may be appropriate for a given system. In completing their analysis, careful consideration should be given to the generic functions performed by the system and the environment in which it operates.

The NIST and NSA are not charged with compliance responsibilities. Reviewers are, therefore, not expected to determine whether or not agencies are complying with the CSA, but for providing comments and suggestions for improving the agencies security planning.

As a first step, the reviewer should read the entire CSPP to obtain an overall perspective on the system and the plan, and ensure that the plan is complete. The reviewer's first impressions of the system and the adequacy of the plan should be recorded at this time. These first impressions should serve as an aid in focusing attention during the detailed review which follows. The summary should consist of no more than one or two paragraphs.

If, during the initial plan review, major sections of the CSPP are found to be missing or seriously deficient, the reviewer should immediately notify his/her team leader. Because of time and resource constraints, review team members are not to contact agencywide or specific system information contacts. Team Leaders are expected to initiate all such contacts, and only in cases where such contacts are ABSOLUTELY ESSENTIAL TO THE PREPARATION OF ANY MEANINGFUL RESPONSE to the submitted materials. Otherwise, the missing or deficient information should be noted in the analysis. A request for resubmission may also be included in the recommendations to the agency.

A.   Part 1 - BASIC SYSTEM IDENTIFICATION

This section of the CSPP should contain basic identifying information about the system.   As indicated above, the purpose of the CSPP is to provide a broad overview of the security and privacy requirements of the subject system and a report of plans for meeting those requirements. This section is not intended to be a detailed technical description of system hardware, content, interconnections, or functions.   It should, however, provide sufficient information to understand the:

--   primary purpose of the system,

--   the generic types of hardware and applications which it supports,

--   the nature of the users,

--   the general operating environment,

--   the generic functions carried out by the system, and

--   any special circumstances which may have a direct bearing on the security or privacy requirements.

The review of this section should focus on the above points. Reviewers should note any areas where insufficient information has been provided and make suggestions for improvement.   If the information provided is too sparse to gain even a minimal familiarity with the nature and environment of the system, it may not be possible to adequately review the following sections on sensitivity and security measures.   In this event, the reviewer should attempt to complete their analysis, noting this situation and highlighting it for special attention during the team leader's preparation of the summary analysis report.

Specific sections required to be contained in this part of the CSPP, and guidance for reviewing their contents are presented below.

Reporting Department or Agency

Self-explanatory

Organizational Subcomponent

A variety of responses may be anticipated here. Generally, a regional office, installation, bureau, or other component of the agency should be specified. Multiple entries may also be expected where the agency has grouped similar systems which are organizationally and geographically distributed. If the latter situation occurs, close attention should be paid to the system description and statement of security requirements to assess the appropriateness of the aggregation.

Where the CSPP is identified as an aggregate planning report (see "Level of Aggregation" subsection, below), the subcomponents

responsible for operating the systems which have been aggregated should be identified in this section.

Operating Organization

Agencies are expected to provide the name of the organizational component or external organization directly responsible for operating the identified system. If this appears to be the name of a contractor or other, non-federal organization, the "Contractor" item should be marked "yes" on the data capture sheet.

System Name/Title

Self-explanatory

System Category

OMB Bulletin 88-16 requires that agencies identify systems as either

-- ### Major Application Systems

These are systems that perform defined functions for which there are clearly identifiable security considerations and needs. Such a system might actually comprise many individual application programs and hardware, software, and telecommunications components.

-- ### General ADP Support System

These consist of hardware and software that provide general ADP support for a variety of users and applications. Individual application systems may be less easily distinguished than in the previous category, but such applications may contain sensitive data. Even if none of the individual applications are sensitive, the support system itself may be considered sensitive if overall, the aggregate of applications and support provided are critical to the mission of the agency.

The identified "System Category" determines which security control list must be addressed by the agency in part 4 of the CSPP. Reviewers should consider whether the category selected is consistent with the description and purpose of the system provided below.

Level of Aggregation

The information processing resource aggregation process is critical to the development of the CSPP and occurs at two distinct points in the plan development process. First, agencies must "draw logical boundaries" around the various processing, communications, storage, and related resources to define a "system" for planning purposes.

Second, rather than have agencies prepare separate submissions for each separate system which has "essentially the same function, characteristics, security needs, and security plans," such systems may be treated as a single system for reporting purposes. This is the aggregation level to be identified under this section.

Such "aggregate" reports are required to be specifically identified. There is NO requirement, however, for agencies to include a listing or other delineation of the number of similar systems which have been aggregated. The reviewer should carefully consider, when reviewing the system description, below, whether systems aggregated for reporting purposes appear to meet the conditions specified above.

Operational Status

Systems must be identified as either:

-- operational, i.e., currently in operation; or

-- under development, i.e., currently under design, development, or implementation.

It should be noted that the operational status of a system can have a substantial impact on the identification and implementation of security controls and protections. Systems may also be operational and under development at the same time, when partial implementation or major modifications are planned.

The operational status of a system can directly affect the ability of the agency to even identify needed controls. For example, a system which is still in the early design stages will almost certainly not have as well documented and complete set of controls and protections as will one that is in the implementation phase. Reviewers should keep the system status in mind throughout their review of the remainder of the CSPP.

General Description/Purpose

This item is key to assessing the appropriateness of security controls identified in Part 3, below, and the appropriateness of filing an aggregated report. Without a reasonable understanding of the purpose and functions of the system (or systems in an aggregate report), evaluating the possible security needs and identifying possible security controls would be impossible.

Agencies are to provide a 1 or 2 paragraph description of the function and purpose of the system. This is NOT intended to be a detailed technical description or a complete functional description of all of the components, subsystems, and processes, or even significant applications which are supported. This description should be judged to be sufficient when it provides the reviewer with a reasonable picture of the nature of the system(s) and the major functions it (they) supports.

In addition to her/his analysis and recommendations with regard to this subsection, the reviewer is expected to select one or more of keywords which capture the nature of the system. (See Chapter III for keyword instructions.)

System Environment and Special Considerations

The physical, operational, and technical environment of the subject system are to be described in this section. Specific items of interest are:

1. The physical and geographic location of the system. Characteristics of the proximate location such as laboratories, central computing facility, mobile or airborne, etc.; and the natural environment such as weightless in space, on the San Andreas fault, north pole, underwater, etc., are important.

2. The types of computer hardware included in the system. It is NOT necessary for agencies to specify the manufacturers or models of their hardware. A generic description such as minicomputers networked using fiber optics, or mainframes supporting a variety of DASD, tape, optical and other peripherals, are acceptable. Care should be taken to note the presence or absence of communications or network hardware.

3. The types of computer software supported by or allowed to be processed on the system should be identified generically. Such characteristics as "off-the-shelf" licensed software performing financial transactions, proprietary contractor developed, in-house developed software, end-user applications, or shareware/freeware should be provided.

4. The nature of the user community should be indicated. Specifically, such characteristics as whether or not the user community includes individuals external to the Government or Government contractors may be extremely important in determining the nature of protections required. Likewise, some indication as to the technical nature or the user community should be provided (i.e., their level of sophistication with regard to computer programming and system operation).

Since the operating environment has a major impact on the risks associated with operating any system, reviewers should give special attention to this subsection. Information provided should be sufficient, combined with that provided under the "General Description/Purpose" subsection, above, to permit the reviewer to gain a general understanding of the operation and use of the system(s) covered by the CSPP, and the resources which have been included in identifying the system(s). Additionally, this subsection should provide sufficient information for the reviewer to make a preliminary judgement as to the appropriateness of an "aggregated report".

Information Contact(s)

Self-explanatory

> **NOTE:** Required contact with the agencywide or system information contact are to be carried out by team leaders.

B.   Part 2 - SENSITIVITY OF INFORMATION HANDLED

Generally, **sensitivity** means the

> characteristic of an asset that implies it is valuable to the organization using it.   It also implies that the asset is vulnerable to accidental or deliberate threats.

The determination of unclassified information sensitivity is a management judgment.   Agencies are expected to use this part of the CSPP to provide a general description of the value of the information, the reasons for the sensitivity, and the areas within which the information may be vulnerable. Agencies should not provide information which is specific or detailed enough that its disclosure would pose a major threat if the CSPP were to be disclosed. Reviewers look for:

-- an overview of the generic types of information handled by the system(s);

-- a general statement of the potential damage which might occur through error, unauthorized disclosure or modification, or unavailability; and

-- a statement of generic threats to which the system or information may be particularly vulnerable.

Sufficient information should be provided to determine the general relevance and potential effectiveness of the security controls specified, when viewed in the context of the system functions and operational environment.

Particular care should be taken by the reviewer to understand the nature of the system sensitivities in light of the foregoing discussions of the functions carried out by the system and the environment in which it operates. It is only the combination of functions, environment, and sensitivity which leads management to recognize requirements to establish security controls.

General Description of Information Sensitivity

Agencies are to provide a general description of the types of information handled by the system and the perceived needs for protective measures.   For example, a budget system identified as a major application might have the following description:

> This system supports budget preparation and analysis activities and process sensitive data related to financial information and applications, commercial information received in confidence, or trade secrets (e.g.: proprietary). Data in this system are most sensitive to inaccuracy or error, and the system is time-critical (i.e., it must be available and produce required results within certain time frames to meet statutory requirements).

Inaccuracy or errors in the data, or unavailability of the system would adversely affect the conduct of agency programs through delaying payments to vendors or employees, and could cause significant damage to the agency's ability to fulfill statutory responsibilities. A major error or unavailability could have an impact on agency operations and activities that could total between $100 thousand and $10 million.

In addition to her/his analysis and recommendations with regard to this section, the reviewer is expected to identify one or more keywords which capture the nature of the

1.   The information processed;

2.   The potential damage which could occur; and

3.   Any generic threats identified.

(See Chapter III for keyword instructions.)

Applicable Laws or Regulations Affecting the System

Any laws or regulations that establish specific requirements for protection of the system or its data or applications should be reflected in this section. Examples might include the Privacy Act, the National Resource Protection Act, the Fair Trade Practices Act, or agency published regulations, such as those directing State governments on the processing of welfare or other benefit payments, specifying requirements for the protection or handling of the information and applications. The Privacy Act, for example, contains requirements for both confidentiality and accuracy of information.

The reviewer is expected to select the code for any identified laws or regulations as shown in Appendix F. Any laws, rules or regulations not shown in the Appendix should be coded as "Other". A title and citation should be provided in the space on the CSPP data capture forms.

System Protection Requirements

Systems processing, storing, or transmitting sensitive information or applications may require protection from:

--   Unauthorized disclosure (confidentiality protection);

--   Unauthorized (including erroneous) modifications which leave data or applications in a condition which is less reliable than that expected by a user (integrity); and/or

--   Unavailability when required (denial of service).

In order to make responsible management judgement relative to cost effective protections that are to be implemented for a sensitive system, agencies must assess the relative importance of the various security controls and protection mechanisms available. This is particularly true where systems process multiple types of information, each of which may have its own particular sensitivities.

The purpose of this section of the system CSPP is to indicate the relative importance of required protections. Specifically, agencies are to indicate for each of the three general categories of sensitivity (confidentiality, integrity, and availability), whether the protection requirements are considered to be **primary**, secondary, or of minimal concern (not applicable).

Reviewers may encounter a variety of presentations for this section. Some agencies may have embedded this determination in the narrative description section, above. Others may provide a simple matrix. Reviewers are to make every effort to identify the sensitivity category(ies) and their relative importance, and code them in the matrix on the analysis summary sheet. It should be noted that more than one of the three categories may be appropriately identified as a "Primary" concern.

While this section represents the agency's management decision about the relative importance of protection requirements, reviewers should consider whether this determination reasonably reflects the functions, environment, identified legal or regulatory requirements, types of information processed, and general sensitivities of the system. This should not be a "second guessing" of agency judgments, but rather a careful expression of concern for the relative priorities which will be assigned system security controls and protections, since this is the only indication provided in the CSPP or the probable level of attention which will be provided to the specific protections.

C. Part 3 - System Security Measures

Having identified the system protection requirements in part 2, above, the agency should identify security measures to address these protection needs. Protections established should be cost effective and based on the specific needs identified in the previous portions of the plan. Agencies are not expected to provide a detailed statement describing the implementation or proposed implementation of the management, procedural, administrative, or technical protections. Rather, OMB Bulletin 88-16 requires that submitted CSPPs indicate:

1. How particular protection measures were decided upon (i.e., formal risk analysis or "other" technique);

2. Any applicable guidance for selecting, designing, implementing, and operating the specific security measures; and

3. The implementation status of the measures by specific control categories.

This part of the CSPP should be reviewed in light of the description of system functions and environment and the identified protection requirements. In particular, each of the control areas specified in OMB Bulletin 88-16 should be specifically addressed in the agency CSPP. The Bulletin provides separate control lists for each of the two types of systems defined OMB 88-16: Major Application Systems and General ADP Support Systems.

Risk Assessment

Agencies are required to indicate whether the specific system protection requirements were established based upon (1) a formal risk analysis, or (2) some other means. If a technique other than a formal risk analysis was employed, the CSPP should include a general description of the procedure or process.

Reviewers should ensure that some indication of the technique used is provided in the CSPP. Their analysis should reflect a judgment as to whether the procedures or technique used appear appropriate for the system and security requirements as described in the previous parts of the plan. Where a technique other than a formal risk assessment has been used, the reviewer is expected to select one or more of keywords which capture the nature of the system. (See Chapter III for keyword instructions.)

Applicable Guidance

Agencies are to indicate, "to the extent practical," specific standards or other guidance used in the design, implementation, or operation of the specified protections. Responses in this section may be expected to vary substantially from system to system and from agency to agency. Reviewers are expected to capture specific Federal or industry standards

on the analysis sheets. Where agency-specific guidance is referenced, this should be indicated and the general category (keyword) recorded on the analysis sheet. (See Chapter III for keyword instructions.)

Review team members and leaders are not expected to be familiar with all of the possible Federal, industry, and international laws, standards, agreements, etc. which might relate to a particular CSPP. However, if the reviewer is aware of possibly applicable Federal, international, or industry guidance or standards not cited by the agency, she/he should cite these materials in the CSPP analysis report and recommendations (e.g. Federal Information Processing Standards (FIPS), American National Standards Institute (ANSI)). Agency specific standards (such as DoD or DoC standards or requirements) should not be referenced.

Security Measure Status

As indicated in the introduction to this chapter, OMB Bulletin 88-16 has identified specific security control areas which are to be addressed in the CSPP. Two specific, different sets of security controls are provided for Major Application Systems and General ADP Support Systems.

The CSPP should indicate for each specific security control whether these measures are:

-- in place for the system;

-- planned for the system, and if so, an anticipated date of implementation;

-- both in place and planned, with specific planned implementation dates for planned measures in the control area; or

-- not applicable for the particular system.

Reviewers should note that it is expected that some agencies will report some specific measures for "operational systems" which are both "in place" and "planned." This may also be true for some measures in systems "under development," although the majority of controls would be expected to be "planned." Additionally, planned controls are expected to be briefly described. (Descriptions may well be limited to the specific description of the security measures included on the OMB 88-16 listings.)

Since there may be many effective techniques for achieving the desired level of protection in a given control area, the CSPPs are not expected to provide sufficient detail for reviewers to determine the appropriateness of security implementations. However, the reviewer should make a general assessment of whether or not the "in place" and "planned " control areas are consistent with the identified system functions, environment and security needs.

The analysis of reported controls should focus on three primary issues:

1. For operational systems, do the indicated controls "in place" appear to address the computer security needs identified in part 2 as associated with the primary sensitivity([1]es) (i.e., confidentiality, integrity, and/or availability)?

2. Will the indicated "In Place" and "Planned" controls address all security needs in areas indicated as primary or secondary?

3. Do the implementation dates for planned controls appear to reflect the priority assigned for those sensitivity areas (i.e., primary, secondary, not applicable)?

Reviewers should provide recommendations regarding control measures included on the OMB Bulletin 88-16 list and their appropriateness for a given system. Recommendations with regard to specific implementations should be avoided.

D.   NEEDS AND ADDITIONAL COMMENTS

This part is provided for agencies to provide additional information with regard to the security of the subject system, and to indicate any needs for specific guidance, standards, or other tools to improve the protection of the subject system.

While no specific analysis of additional information provided in this section about the security of the subject system is required, it should be reviewed carefully to enable the reviewer to gain a better understanding of the system and related protection requirements. Whenever specific needs for additional guidance, standards, or other tools, are identified, the reviewer should mark a "4" on the CSPP jacket, in order to alert the Project Managers.

VII. <u>PREPARING THE SUMMARY ANALYSIS AND RECOMMENDATIONS</u>

The team leader is responsible for preparing the final agency summary analysis and recommendations. This document should be limited to 2 to 3 pages, and should summarize the analyses and recommendations relating to the agency's program overview and the CSPPs. This summary provides a mechanism for focusing the agency's attention on significant computer security planning issues which may have an impact across agency systems.

Specifically, the summary should address the following issues:

1. If no program overview was submitted, determine if there is a substantial disparity in overall approach or specific controls in place or to be implemented for similar systems and environments among the CSPPs submitted. This could indicate a lack of clear policy, guidance, and requirements within the agency.

2. If a program overview was submitted by the agency, determine if the CSPPs appear to be consistent with the program as outlined in the summary, as well as consistent with each other (i.e., there should not be a noticeably wide disparity in the approach taken).

3. If a significant number of plans submitted are for operational systems, determine whether the majority of controls are "in place" or "planned". A large number of planned controls for operational systems may indicate weak computer security planning activity during the design, development, and testing of systems.

4. If no agency program overview was submitted this may (or may not) indicate that the agency has no comprehensive computer security program. The essential elements of such a program (see Chapter V) should be briefly restated.

5. Significant problems (or potential problems) which were consistently identified in CSPP reviews should be highlighted and any recommendations for agencywide actions to address the problem should be included in the summary.

APPENDIX E

OMB BULLETIN 89-17
FEDERAL INFORMATION SYSTEMS AND TECHNOLOGY PLANNING

THE DIRECTOR

August 22, 1989

BULLETIN NO. 89-17

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

SUBJECT: Federal Information Systems and Technology Planning

1. <u>Purpose</u>. This Bulletin provides guidance and instructions to selected agencies for the preparation and submission of information on their strategic plans for information systems and technology. It also requires all agencies to update the designations of senior officials for Information Resources Management pursuant to Section 3506 of Title 44 U.S. Code and Section 9(a)(9) of OMB Circular No. A-130.

2. <u>Authority</u>. This Bulletin is issued pursuant to the Budget and Accounting Act of 1921, as amended; the Budget and Accounting Procedures Act of 1950, as amended; and the Paperwork Reduction Act of 1980, as amended.

3. <u>Background</u>. The 1986 amendments to the Paperwork Reduction Act provided that each agency shall "develop and annually revise a five-year plan, in accordance with appropriate guidance provided by the Director, for meeting the agency's information technology needs." In addition, OMB Circular No. A-130, "Management of Federal Information Resources" (December 12, 1985), provides that agencies shall "[e]stablish multi-year strategic planning processes for acquiring and operating information technology that meet program and mission needs, reflect budget constraints, and form the basis for their budget request." Such plans are necessary to:

- Improve agency management by providing timely information to support decision-making and to forecast resource and system requirements.

- Support government-wide planning and oversight by providing consistent and complete information concerning major information systems and technology investments.

The information requested by this Bulletin will be used for several purposes:

- To encourage effective planning by Federal agencies;

- To provide information on Federal information systems and technology plans to Congress and the public through "A Five-Year Plan for Meeting the Automatic Data Processing and Telecommunications Needs of the Federal Government";

-   To provide information for the annual budget review
    process; and

-   To support analysis and development of Federal information
    resources management policies.

Information submitted shall be consistent with the 1990 Budget.

4.   The Computer Security Act of 1987.   The Computer Security Act
of 1987 (Public Law 100-235) established a number of requirements
to assure the security of Federal computer systems that process
sensitive information.

-   By July 8, 1988, agencies were to identify those Federal
    computer systems within or under their supervision that
    contain sensitive information;

-   By September 6, 1988, agencies were to begin a security
    awareness and training program pursuant to regulations
    issued by the Office of Personnel Management (OPM);

-   By January 8, 1989, agencies were to develop computer
    security plans and submit them to the National Institute
    of Standards and Technology and the National Security
    Agency for advice and comment; and,

-   A summary of the agency's security plans shall be included
    in the agency's five-year information technology plans.

In addition to incorporating computer security planning in the
agency five-year planning process, agencies are required by this
Bulletin to submit summaries of their computer security plans for
publication in the government-wide five-year plan.

The terms "computer system," "Federal computer system," and
"sensitive information" are defined in Public Law 100-235.
Agencies should note that Federal computer systems include
contractor, State, and local government computer systems that
process information on behalf of the Federal Government to
accomplish a Federal function.

5.   Definitions.   For purposes of this Bulletin, the following
definitions apply:

a. The term "information resources management" means the
planning, budgeting, organizing, directing, training, promoting,
controlling, and management activities associated with the
burden, collection, creation, use, and dissemination of
information by agencies, and includes the management of
information and related resources such as automatic data
processing equipment (as such term is defined in Section 111(a)
of the Federal Property and Administrative Services Act of 1949
(40 U.S.C. 759(a)).

b. The term "information technology" means the hardware and software used in connection with government information, regardless of the technology involved, whether computers, telecommunications, micrographics, or others. For the purposes of this Bulletin, automatic data processing and telecommunications activities related to certain critical national security missions, as defined in 44 U.S.C. 3502(2) and 10 U.S.C. 2315, are excluded.

c. The term "major information system" means an information system that requires special continuing management attention because of its importance to an agency mission; its high development, operating or maintenance costs; or its significant impact on the administration of agency programs, finances, property, or other resources.

d. The term "major information technology initiative" means an agency project to install, automate or modify a major information system, for which the cost of system development and acquisition (including aggregated totals of like items such as microcomputers) from conception through implementation will exceed $25 million or the cost in any year will exceed $10 million.

The term "major information technology initiative" includes investments in hardware, software, and telecommunications. It also includes actions that are part of the planning stage; e.g., feasibility studies of automation alternatives, benefit-cost analyses, needs assessments, or technology evaluations that may result in a new major information system or substantial modification to an existing major information system.

e. The term "strategic planning" means a process of defining agency missions and identifying agency goals, objectives and activities over a specified period of time. With respect to information systems and technology, strategic planning means specifying the application of information technology and other information resources to support identified missions and objectives.

6. Changes from Previous Years.

a. Updated designation of senior official for information resources management. Agencies are asked to provide a letter, signed by the agency head, identifying the agency's senior official for information resources management as provided for in the Paperwork Reduction Act. Many of these officials have changed with the change of the Administration.

b. Strategic Overviews and Summary of Computer Security Plans (Appendix A). Agencies are asked to include, as a part of their strategic overviews of agency information technology plans

-3-

and priorities, a summary of their computer security plans, as provided for in the Computer Security Act of 1987.

    c. <u>Policy Analysis on Image Processing Systems (Appendix B)</u>. Last year's requirement for descriptions of projects to create or expand electronic mapping databases is deleted. The results of that initiative are described in Volume II of the 1988 <u>Five-Year Plan for Meeting the Automatic Data Processing and Telecommunications Needs of the Federal Government</u>. A new requirement is added for information on projects to develop image processing systems, in order to compare performance requirements and standards and to identify opportunities to share experience and expertise among agencies.

    d. <u>Policy Analysis on Electronic Data Interchange (Appendix C)</u>. A new requirement is added for information on agency initiatives to convert business and financial transactions from paper to electronic form, known as electronic data interchange. The information collected will be used to establish goals and priorities, and to develop a baseline from which to measure progress.

7. <u>Coverage</u>. <u>All agencies are required to establish appropriate information technology strategic planning processes and to submit updated designations of senior officials in accordance with paragraph 8.a below</u>. The following agencies are subject to the reporting requirements of this Bulletin enumerated in paragraphs 8.b, 8.c, and 8.d.

Department of Agriculture
Department of Commerce
Department of Defense
Department of Education
Department of Energy
Department of Health and Human Services
Department of Housing and Urban Development
Department of the Interior
Department of Justice
Department of Labor
Department of State
Department of Transportation
Department of the Treasury
Department of Veterans Affairs
Environmental Protection Agency
General Services Administration
National Aeronautics and Space Administration
Office of Personnel Management
Small Business Administration
National Archives and Records Administration
Federal Emergency Management Agency
National Science Foundation
Nuclear Regulatory Commission
Railroad Retirement Board

United States Information Agency
Agency for International Development
Federal Communications Commission

8. <u>Action Required</u>. Not later than 10 weeks from the date of issue, each department and agency listed in paragraph 7, above, shall submit the following to: S. Jay Plager, Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget, 3235 NEOB, Washington, D.C. 20503, in one paper copy:

    a. A letter, signed by the head of the agency, identifying the official who has been assigned pursuant to 44 U.S.C. 3506(b) to serve as the senior official for Information Resources Management. If the head of the agency has designated the senior official to a particular position by regulation or order, a copy of the regulation and the name of the current incumbent in the position so designated will suffice.

    b. An agency strategic overview in accordance with instructions in Appendix A. This will identify accomplishments in, and planned initiatives for, the improvement of agency information resources management. The overviews will be published in the government-wide Five-Year Plan.
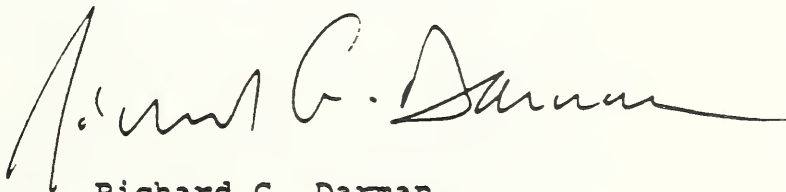
In addition to the paper copy of this submission, agencies should submit one single-spaced ASCII version (65 character line length) on a 5 1/4" (double-sided) or 3 1/2" double-density soft-sectored diskette.

    c. Discussions of image processing initiatives, if applicable, in accordance with instructions in Appendix B.

    d. Discussions of EDI initiatives, if applicable, in accordance with instructions in Appendix C.

9. <u>Information Contact</u>. Questions regarding a specific agency's submission should be directed to the Desk Officer in OMB's Office of Information and Regulatory Affairs who reviews that agency. Questions regarding electronic submission should be directed to Robert Veeder (395-4814). Questions of a more general nature may be directed to Bruce McConnell (395-3785).

10. <u>Sunset Date</u>. This Bulletin expires March 31, 1990.

Richard G. Darman
Director

Attachments

-5-

INSTRUCTIONS FOR PREPARING AGENCY STRATEGIC OVERVIEW
INCLUDING SUMMARY OF COMPUTER SECURITY PLANS

General. The purpose of the strategic overview is to describe
the program priorities of the head of the agency and to discuss
how information technology is being used to meet those
priorities. In addition, it seeks to identify specific ways
agencies are improving, or are planning to improve, the
management of their information resources pursuant to 44 U.S.C.
3514 (a)(9)(A). This information should not exceed eight double-
spaced pages, and will be published in the 1989 Five-Year Plan.

Content. The strategic overview is a narrative with three
individual sections captioned as indicated below:

-   Summary. Describe the agency's program priorities and
    explain how agency plans for information systems and
    technology will support those priorities over the next 5
    years. Discuss major changes the agency has made in FY
    1988 in its planning for information technology resources
    and any anticipated changes it will make in the next 5
    years. Explain the assumptions the agency is making about
    changes in its programs and the policies governing them.

-   Accomplishments and Initiatives. Describe specific FY 1988
    accomplishments in the improvement of, and planned general
    management initiatives to improve, information resources
    management in the agency. Agencies may also describe more
    recent accomplishments if the information is readily
    available. Particular attention should be given to
    describing how agency activities will improve the delivery
    of services to the public. Include brief descriptions both
    of policy initiatives and of major information technology
    initiatives. Relate these accomplishments and initiatives
    to the agency's program priorities. In particular,
    agencies should tie planned initiatives to the policy
    priorities identified by the agency head in response to the
    President's Memorandum of April 11, 1989 to the Heads of
    Executive Departments, the National Aeronautics and Space
    Administration, and the Environmental Protection Agency --
    "Management by Objectives." Discuss the scope of the
    accomplishment or initiative, i.e., whether the effects
    were or are agency-wide or bureau- or system-specific, any
    reduction of burden on the public, and any quantitative
    measures of improved efficiency in the collection,
    creation, use or dissemination of information. Discuss
    associated milestones and timeframes, where applicable.

- <u>Summary of Computer Security Plans</u>. Summarize the computer security plans submitted to the National Institute of Standards and Technology and the National Security Agency for advice and comment pursuant to the Computer Security Act of 1987. Include a brief description of:

-- <u>Changes in policies</u>. Describe any changes in security policy within the agency to implement the Computer Security Act of 1987.

-- <u>Improvements in the security of systems to date</u>. Describe changes in the security of the most sensitive Federal computer systems that process unclassified information which have been implemented during the past year.

-- <u>Personnel awareness and training activities</u>. Describe the agency's computer security awareness and training program. Discuss how the implementation of awareness and training is being monitored. By what date will all end users, managers and technicians who are involved with computer systems that contain sensitive information receive security and awareness training?

-- <u>Agency-wide security priorities</u>. Describe planned priorities (<u>e.g.</u>, contingency planning, communications security, access controls, application software quality control) to improve security agency-wide which result from agency assessment of the computer security plans provided to NIST and NSA.

-- <u>Material weaknesses</u>. Describe generally key material weaknesses that have been identified under OMB Circular No. A-123 and the Federal Managers Fiscal Integrity Act.

-- <u>Actions to assure implementation of security plans</u>. Describe agency plans and activities to assure that system computer security plans are implemented and that material weaknesses are corrected, including any funding and oversight mechanisms to be used.

Format. (sample)

DEPARTMENT OF GOVERNMENT

STRATEGIC OVERVIEW

Summary: _____

_____
_____
_____

Accomplishments and Initiatives: _____

_____
_____
_____

Summary of Computer Security Plans: _____

_____
_____
_____

    -- Changes in policies: _____

_____
_____
_____

    -- Improvements in the security of systems to date. ____

_____
_____
_____

    -- Personnel awareness and training activities. _____

_____
_____
_____

    -- Agency-wide security priorities. _____

_____
_____
_____

    -- Material weaknesses. _____

_____
_____
_____

    -- Actions to assure implementation of security plans. __

_____
_____
_____

INFORMATION ON INVESTMENTS IN IMAGE PROCESSING SYSTEMS

General: The purpose of this information request is to identify projects which are designed to put paper documents into optical image systems. Agencies are finding that it is increasingly cost-effective to develop these systems to handle and store information which has previously been on paper. However, requirements for speed of retrieval, level of accuracy of images, legal status of image records, and image storage formats are not widely agreed on and a number of parallel development efforts are underway. The results of this survey will be used to compare performance requirements and standards, to identify opportunities to share experience and expertise among agencies, and to publicize projects which may have value beyond the sponsoring agency.

Definition: For the purposes of this Appendix, optical image systems electronically convert, store in digitized form, process, manipulate, and retrieve (to screen or in printed form) information originally created on paper. These systems preserve the essential visual and spatial characteristics and appearance of the original (on paper) information, including handwriting, drawings, form designs, and other non-standard input.

Facsimile machines used solely to transmit documents and microfiche systems are not included.

Coverage: The information requested below shall be provided:

1. For each project where the expected cost exceeds $1 million in one fiscal year, or $3 million during fiscal years 1989-1993.

2. For smaller, precedent-setting prototype projects, which the agency believes may lead to larger systems in the future.

Content: For each project, report the following information:

1. Name of the project, and a description of the purpose and scope.

2. Mission requirement the system is designed to satisfy.

3. Estimated costs (capital investment and operations) for each fiscal year 1989-1993.

4. Description of input (typewritten text, invoices, receipts, forms, drawings, etc.). If practical, attach examples of documents that illustrate the various types of information that

will be captured. For example, if documents contain both text and image, provide a sample of that type of document.

5. Description of the origin of the input including both the type and location of organizations supplying the documents and the technology that the supplier uses to create the documents, if known.

6. Description of the conversion and input process, including scanning system, authentication procedures, use of outside contractors, quality control and data loading procedures.

7. Proposed accuracy of stored image (150 dots per inch, 200 dots per inch, etc.).

8. Storage format for images (Group 4 FAX, etc.).

9. Description of proposed work station for retrieval (including screen resolution, number and size of screens, communications speed and protocol, zoom, local storage capacity, etc.).

10. Volume of stored images (in pages and bytes) to be captured initially, total volume online each year FY 1989-1993, volume removed from online access (archived or destroyed) each year FY 1989-1993.

11. Response time for online document retrieval.

12. Brief description of the operation of the indexing and storage system (index keys, searching techniques, off-the-shelf system, etc.).

13. A description of unique functions, capabilities, or performance standards (such as large format hardcopy output, grey scale image enhancement, etc.) required by this system that will make it different from commercially available systems.

14. The name and telephone number of a point of contact who can provide more information.

INFORMATION ON ELECTRONIC DATA INTERCHANGE

General. The purpose of this information request is to establish
a baseline for measuring progress in the conversion of financial
and business transactions from paper to electronic form. The
baseline will be used to establish goals and priorities for the
government in electronic data interchange.

Definition. For purposes of this Appendix, electronic data
interchange (EDI) means the conversion of business information
from paper to a standard electronic format, and the transmission
of that information between industry and the Federal Government
using a magnetic tape diskette, or communications facilities.
Business information includes the full range of information
associated with high volume, repetitive, commercial and business
transactions. Examples include:

o   financial transactions, such as invoices, remittances and
payments, entitlement benefit transfers, payment status
inquiries, and payment cancellation requests;

o   procurement and contract transactions, such as price/sales
catalogs, requests for quotations, invitations for bid, requests
for proposals, specifications, bids, offers, proposals, trading
partner profiles, notices of contract solicitation and award,
purchase orders, contract documentation deliverables,
regulations, market research data, debarment data, shipping
manifests, bills of lading, planning/availability schedules,
shipment status reports, change orders, reports of test results,
safety data, warehouse activity reports, service history, and
warranty data; and,

o   regulatory transactions, such as tariff filings, tax
information and filings, and customs and import/export
declarations.

Content. Provide a list of each existing and planned EDI
initiative showing:

1. name of the project and a description of the purpose and
scope;

2. mission requirement that the initiative is designed to
satisfy;

3. a description of the transactions being converted;

4. the date (or proposed date) of actual implementation;

5.   the estimated number of organizations that will use EDI:
(a) Federal; (b) industry/private. If practical, estimate what
portion of private users are small businesses;

6.   the estimated number of transactions per year (e.g., number
of invoices), and the target percentage that will be EDI for each
of the years FY 1990-94.

7.   a brief discussion of the estimated costs and benefits of
implementing the project;

8.   the standards used (e.g., ASC-X12, EFT (specify), EDIFACT,
TDCC, UCS, agency-specific);

9.   the method for transmitting the information (e.g., floppy
disk, tape, telecommunications). If telecommunications are used,
be specific (e.g., dial-up over voice line, X.25 via value-added
network, X.400 electronic mail);

10. significant problems or interesting solutions associated with
this initiative, if any; and

11.   the name and telephone number of a point of contact who can
provide more information.

APPENDIX F

ABBREVIATIONS AND ACRONYMS

5. the estimated number of organizations that will use EDI:
(a) Federal; (b) industry/private. If practical, estimate what
portion of private users are small businesses;

6. the estimated number of transactions per year (e.g., number
of invoices), and the target percentage that will be EDI for each
of the years FY 1990-94.

7. a brief discussion of the estimated costs and benefits of
implementing the project;

8. the standards used (e.g., ASC-X12, EFT (specify), EDIFACT,
TDCC, UCS, agency-specific);

9. the method for transmitting the information (e.g., floppy
disk, tape, telecommunications). If telecommunications are used,
be specific (e.g., dial-up over voice line, X.25 via value-added
network, X.400 electronic mail);

10. significant problems or interesting solutions associated with
this initiative, if any; and

11. the name and telephone number of a point of contact who can
provide more information.

APPENDIX F

ABBREVIATIONS AND ACRONYMS

APPENDIX F
ABBREVIATIONS AND ACRONYMS

ABBREVIATION OR ACRONYM	MEANING
A&A	Authorization/Access Controls
Act	Computer Security Act of 1987 (same as PL 100-235 or CSA)
ADP	Automated Data Processing
AF	Air Force
AIS	Automated Information System
Anal	Analysis
Assignmt	Assignment
Aud Var	Audit and Variance Detection
Authoriz(atn)	Authorization
Brd	Board
CAB	Cabinet
Cert	Certification/Accreditation
Compl	Compliance
Conf	Confidentiality Controls
Conting	Contingency
CSO	Computer Security Officer
CSPP	Computer Security and Privacy Plans
Ctls	Controls
DBMS	Data Base Management System
Doc	Documentation
DoD	Department of Defense
DR&T	Design Review and Testing
Emer	Emergency, Backup and Contingency Plans
Emerg	Emergency
Envir Protect	Environmental Protection
GADPS	General Automated Data Processing Support
Gov't	Government
I/O	Input/Output
IEEE	Institute of Electrical and Electronic Engineers
Inc.	Incorporated
IND	Independent
Int	Integrity Controls
IRM	Information Resource Management
ITR	Information Technology Resource
JUD	Judicial
LEG	Legislation
MAS	Major Application System

ABBREVIATION OR ACRONYM	MEANING
MIN	Minimal
Mini	Minicomputer
Misc	Miscellaneous
N/A	Not Applicable
NBS	National Bureau of Standards (former designation of the National Institute of Standards and Technology)
NCSC	National Computer Security Center
NIST	National Institute of Standards and Technology (formerly the National Bureau of Standards or NBS)
Non-aggreg	Non-aggregated
NSA	National Security Agency
OMB	Office of Management and Budget
Oper & Und	Operational and Under development
Oper	Operational
OPNAVINST	Operation Navy Instruction
PC	Personal Computer
Pers	Personnel Selection/Screening
Persn	Personnel
Phys	Physical and Environmental Protection
PL 100-235	Public Law No. 100-235 (same as CSA or ACT)
PRI	Primary
Prod	Production(, I/O Controls)
Prot	Protection
Reg	Regulation
Resp	Assignment of Security Responsibility
Respon	Responsibility
Risks	Risk/Sensitivity Assessment
S/W	System Software Controls
SAT	Security Awareness and Training
Sec	Security
SEC	Secondary
Secur/AcquisSpecs	Security/Acquisition Specifications
Sel	Selection
Spec	Special
Sys S/W & Maint	System Software and Maintenance
Sys	System
Telecom	Telecommunications
TIS	Trusted Information Systems, Inc.
Und Devel	Under Development
US	United States
Userid	User Identification
Va	Variance

APPENDIX G

APPLICABLE LAWS AND REGULATIONS AS REPORTED BY CSPPs

APPENDIX G
APPLICABLE LAWS AND REGULATIONS
AS REPORTED BY CSPPs

In some instances the same documents may be referenced under different names. In some cases items which should have been approprietely identified under Applicable Guidance were reported by some CSPPs in this catagory. See Appendix H, Applicable Guidance as Reported by CSPPs.

ACS Dir: Financial Man. Sys.
Adams vs. Bennett
Administrative Procedures Act
ADP Security Manual DM 3140
Agr. Act of 1970, Sec. 812
Agr. Trade Dev.& Assist. Act
Agr. Marketing Act of 1946
Agr. Adjustment Act of 1938
Agr. Credit Act of 1987
American Antiquitors Act
Antitrust Civil Process Act
Arch. Resource Protection Act
Arch. Recovery Protection Act
Atomic Energy Act
Brooks Act
Buckley Amend. to Privacy Act
Budget Reform Act of 1988
Budget and Acc. Act of 1950
Budget and Acc. Act of 1921
California Info. Practices Act
Cash Management Act
Chapter 11, Bankruptcy Code
Civil Rights Act of 1964
Classification Act
Class. and Prot. of RSMS Meas.
Clayton Act
Clean Drinking Water Act
Clean Air Act
Commodity Exchange Act
Competition in Contracting Act
Drug Abuse Prev. & Control Act
Compre. Crime Control Act
Comp. Fraud & Abuse Act of 1986
Cong. Budget & Imp. Control Act
Consumer Product Safety Act
Controlled Substance Act
Copyright Act of 1980
Crime Control Act of 1984.
Debt Collection Act of 1982
DOE 5400.xy
DOT/FAA Order 1600.15B
DOT/FAA 1300.22A
Ed. Dept. Risk Manag. Handbook
Ed. Dept. Acquisition Regs.
Education Amendment of 1972
Endangered Species Act
Executive Order 10450
Executive Order 11490
Executive Order 12356
Executive Order 12352
Executive Order 12291
Executive Order 11478
Executive Order 12498
Explosives Control Act

Export Administration Act
Fair Credit Reporting Act
Fair Trade Practices Act
Federal Reports Act
Fed Prop & Admin Services Act
Fed Prop Man. Regs Temp.
Fed Financial Integrity Act
Fed Code of Regs Part 7 - Agr.
Fed Power Act
Fed Credit Union Act of 1954
Fed Rules of Criminal Procedure
Fed Debt Recovery Act
Fed Oil&Gas Royalty Man. Act Fed Land Policy & Man. Act
Fed Personnel Manual
Fed Property Management Regs
Fed Info Resources Manag Regs
Fed Trade Commission Act
Fed Computer Crime Act of 1984
Fed Hazardous Substance Act
Financial Privacy Act
Financial Manag. Integrity Act
Fiscal Procedures of GAO Manual
Fish&Wildlife Coordination Act
Flammable Fabrics Act
Food Stamp Act of 1964
Foreign Corrupt Practice Act
FPM Chapter 296, 297, 432, 531
FPM Chapter 451, 731, 732, 736
FPM Chapter 754, 771, 751
Freedom of Info Act of 1974
GAO ORDER 2713.6, 0920.1
GAO Policy and Proc. Manual
GAO Privacy REGS
GPO Instruction 825.16A
Telecom and AIS Sec. Program
Gramm Rudman Act
Gun Control Act
Antitrust Improvements Act
HHS Standards of Contact Regs
Indian Land Leasing Act of 1909
Indian Mineral Development Act
Integrity Act
International Traffic in Arms

Reg
Interior Prop. Management Regs
Internal Revenue Code
Invest. Manag. Co. Act of 1940
Investment Advisor Act of 1940
Land Management Planning Act
Fisheries Conserv. & Manag Act
Marine Mammal Protection Act
Meat Import Law (P.L. 96-177)
Mineral Leasing Act
NASA, JPL Comp Sec Requirements
Nat'l Cooperative Research Act
Nat'l Credit Union Act of 1934
Nat'l Environmental Policy Act
Nat'l Firearms Act
Nat'l Historic Pres. Actof 1966
National Housing Act, 1934
Nat'l Resource Protection Act
Nat'l Forest Management Act
Natural Gas Policy Act of 1978
OCS Lands Act
Official Procedures Policy Act
OMB Circular A-91
OMB Circular A-129
OMB Circular A-130
OMB Circular A-123
OMB Circular A-102
OMB Circular A-10
OMB Circular A-11
OMB Circular A-110
OMB Circular A-122
OMB Circular A-125
OMB Circular A-127
OMB Circular A-21
OMB Circular A-50
OMB Circular A-71
OMB Circular A-121
OMB Circular A-87
OMB Circular A-73
OMB Circular A-109
Omnibus Trace & Compet. Act
OPM FPR Chapter 731, 732
OSHA Act
Paperwork Reduction Act

1

PL 99-500 PL 100-235,
PL 73-479 PL 94-492,
PL 93-502 PL 96-511,
PL 100-297 PL 100-323,
PL 92-484 PL 93-1055,
PL 93-502 PL 93-577,
PL 97-365 PL 95-452,
PL 98-369 PL 98-473,
PL 100-456 PL 99-474,
PL 96-511, PL 98-473
PL 100-225, PL 91-508
PL 93-110 (31 USC 5315)
PL 94-472, PL 93-259
PL 93-579, PL 93-599
PL 95-277, PL 99-198
Poison Prev Packaging Act
Privacy Act of 1974
Pub Util Holding Co Act of
 1935
Railroad Retirement Act
RR Unemployment Insurance
 Act
RR Reutilization & Reform
 Act
Records Manag by Fed
 Agencies
Refrigeration Safety Act
Refugee Education Assist Act
Regulatory Flexibility Act
Resource Planning Act
Right to Financial Privacy
 Act
Securities Act of 1933
Securities Exchange Act of
 1934
Small Business Act
Social Security Act
Supp. for Pollution
 Abatement
Sur. Mining Cont & Reclam
 Act
Tariff act of 1930
Tax Reform Act
The Staggers Act of 1975
Toxic Substances Control Act
Trade and Tariff act of 1984
Trade agreements act of 1979
Trade Secrets Act of 1905
Trade Act of 1974
Traffic Act of 1930
Treasury Rules and Regs
Treaty on Narcotic Drugs
Trust Indenture Act of 1939
US Grain Standards Act
USDA ADP Security Manual
VA ADP Policies and
 Handbooks
Welfare Laws
Wire & Ele Com Interception
Witness Security Reform Act
 of 1984.
Witness Protection Act
10 USC 60
12 USC 95a, 22 USC 5315
13 USC (Nat. sec. Info.)
15 USC 1151-1157
15 USC 176a
18 CFR 128, 161, 250, 284,
18 USC 1906
18 USC 2351
18 USC 2510
18 USC 1902
18 CFR 35.13, 270, 273,
18 CFR 154.38, 154.63, 521
18 CFR 157, 260, 385, 388
18 USC 1030

18 USC 2071
18 USC 1905, 1906
18 USC 641
18 USC 1343
18 USC 3500, 3521
18 USC 751-75
18 CFR 11, 154.301, 154.310
18 USC 1030(A)(4)
18 USC 2511
26 USC 6103
28 USC 569.
31 USC 5311
35 USC Sec. 181-188
36 CFR Subchapter E
38 USC
4 CFR 81, 83
40 USC 483(b)
44 CFR Chapter 22
44 USC 3501
44 USC Section 3508
44 USC 3501-3520
49 CFR Part 12, 44
5 USC 301
5 CFR Part 351
MP-1, MP-2, MP-3, MP-4, MP-5
MP-1-76, MP-6
MP1 PT1 5
MP1 PT2 13
NMI 1382.17
NMI 1382.17B
NMI 1620.7
NMI 2410.7A
NCSC 11
NSDD 145
NSDD 97
NTIS #2
NTISS # 2
NTISS # 200
NTISS 3005
NTISSP 2, 200

APPENDIX H

APPLICABLE GUIDANCE AS REPORTED BY CSPPs

APPENDIX H
APPLICABLE GUIDANCE
AS REPORTED BY CSPPs

In some instances the same documents may be referenced under different names. In some cases items which should have been approprietely identified under Applicable Laws and Regulations were reported by some CSPPs in this catagory. See Appendix G, Applicable Laws and Regulations as Reported by CSPPs.

Departmental OIRM LAN
 reference guide
NASA G/Ls for Devel of
 CompuSec Train Pgms
NASA G/Ls for Safeguarding NASA
 Sensitive Systems
NASA ADP Risk Analysis G/Ls
NASA G/Ls - Certifying Sens.
 Appl.
NASA G/Ls - Contingency
 Planning
NASA Scientific and
 Technical Information
 Handbook
Systematic Software Devel &
 Maintenance Boeing CO.
10 CFR, 40 CFR (EPA)
29 CFR (DOL), Occupational
 Safety and Health
3Com 3Plus Network
 Administrators Guide
42 CFR Part 60, Health Ed
 Assistance Loan Program
ACS Directive: The Financial
 Management System
ADABAS Application Devel
 Procedures Manual
ADABAS Natural Security
 Product Procedures
ADP Equip Acq Plan
ADP Security Manual (DM
 3140-1)
ADP Security Policy & G/Ls
 circular
ADP Security Standards
ADPE Fips Pub
ADPF DOE Safety and Security
 Reg
AF Regulation 205-16
AID IRM Standards/Policy
AIMS User's Guide
ALLIED Corporation Policy
 and Security Standards
Approved Industry Procedures
ASCD Handbook "Automated
 Systems Security"
ASCS Handbook "ADP Security
 Admin Handbook"
Audit Standards
Account Data Group
Advanced Netware/68 Users
 Guide
Agency Policies
Agency Regs
Agency admin directives
 1350, 1355, 1360
Applicable Fed Standards
OCC Application Devel Life

Cycle STDs
Applications G/Ls
BEA SOP
BEP Circular #71-00.19
BES Customer Handbook
BLM Manuals
BPA Information Management
 Security Manual
CAS Accounting/procedures/
 manual
CAS Guide to ADP Application
 Control Procedures
CDPA Secure OPS Handbook
City building ordinances
Combination of Fed and
 Industry standards
Contractor supplied software
 Copyright law
CSC-STD-001-83
Census Administrative Manual
Census Computer Handbook
Census Computer User's Guide
Census Manuals
Center SOP's
Center-level site-specific
 documents
Circular 10-88-78
Classification and
 Protection of RSMS
 Measurements
Code of Fed Regulations
DOC Criteria for Resol. of
 Intrnl Ctrl Weakness
DOC Info. Tech. Handbook
DOC Methodology for
 Certifying Sens. Appl.
DOC Security Manual/Handbook
 of Security Regs
Commercial Product-PC
 Guardian
Common Sense
Communications Act of 1934
Computer Access Management Plan
Computer Security Handbook
Computer Security
 Requirements-CSC-STD-003-85
Computer Security Symposium
Contractor Recommendations
Contractor site-specific
 documents
D&MS Circular 1-88-78
DCAZ 630-230-19
DCID 1/21
DEA Charter
DHHS & PHS Chapters in Gen
 Admin Manual
DHHS ADP Systems Manual
 (Part 6)

DHHS Accounting Procedures
DHHS IRM Manual
DIRM Internal Control
 Procedures
DIS Regs 20-12, 21-3, 25-2,
 31-4
DLAH 4730.1
DLAM 4215.1, 5200.1, 7000.1
DLMS sections
DM & S ADP Security Policy
DNA Inst 5200.28C
DOB Order 2640.2A AIS
 Security
DOB-M-20-4
DOC Resolution of Material
 Internal Control Weakness
DOC Info. Tech. Handbook
DOC Info. Management
 Handbook
DOC Info. Technology
 Security Manual
DOC Methodology for Cert.
 Sens. Appl.
DOC Nat. Security Info
 Manual
DOD password management G/L
DOD pubs
DOD Trusted CS Eval
 Criteria, CLASS C2
DODCI Computer System
 Security Course class notes DOE
13160.2A
DOE ADPE Acquisting P.L.
 83-DO3
DOE and Safety and security
 rights
DOE internal control
DOE orders, policies, guide,
 regs
DOE safety & security regs
DOE unclass computer
 security G/LS
DOJ Guidance for Conducting
 a Risk Analysis
DOJ orders
DOJ Order AIS Security &
 Policies
DOJ Order Security Pgms &
 Responsibilities
DOJ Order Safeguarding Grand
 Jury Info
DOJ Order Safeguarding Tax
 Returns & Info
DOJ Control & Protection of
 Limited Official Use Info
DOJ Order Security Regs for
 Systems of Records
DOJ Order Correspondence

Procedures
DOJ Order IRM Program
DOT 5200.28-STD
DOT CPMIS and Operations
 Users Manual
DOT G/Ls
DOT Internal Policies,
 Regulations & Orders
DOT Personnel Users Manuals
DOT/OIG Operating Procedures
 Manual
DPI G/LS (MSFC #6218)
DR 3140-1 ADP Security
 Policy
Draft EPA Information
 security manual 1988
DSN DOC 810-39, DSN Computer
 & Data Sys Security
DSN DOC 820-20, Deep Space
 Network Gen Req. & Policies
DTICR 5230.3
DTSA Admin Instruction 18
DVB-M20-4
Debt Collect Act of 1982
Defense Criminal Investigative
Service Agent
 Manual
Dept of State security STDS
 for unclassified AIS
Dept of State Foreign
 Affairs Manual
Dept of State System
 Security Standards #'s
 4 & 5
Dept's ADP Risk Management
 Handbook
Dept's ADP Security Manual
Dept's Life Cycle Management
 Manual
Dept's Regulation 3140-1
Dept'al ADP Stds
Dept'al Accounting Manual
Dept'al Directive on "Internal
Control Reviews"
Dept Reg 1042-42 - Crop
 Reports
Dept of State Foreign
 Affairs Manual
Dept of Interior Manuals 350
 DM3-350DM5, 351 DM7-352DM6
Determined by FAA
Disaster Recovery Plan
Diskette Specs & Formats for
 50059 & 52670 data
 submission
DoD 5106.1, 5200.28-STD,
 5400, 7110, 7950.1-M, Std
 5200.25
DoD Directive 5400-11-4
DoD Password Management
 G/L-CSC-STD-002-85
DoD Trusted Computer Eval.
 Criteria-CSC-STD-001-85
DoDD 4100.39-M, 4160.21-M,
 5200.28
E.O. 10450
EAP OIRM system design and
 Devel Guidance
EEE Ethernet Specifications
EG&G derived STD &
 Procedures document, August
 1986.
EPA Acquisition Regs
EPA Contracts Mgmt Manual
EPA IRM Policy & Privacy Act
 Manual

EPA Regulation on
 Confidential Business Info
EPA SYSTEM DESIGN & Devel
 GUIDANCE
ESS ADP Security Plan
ESS ADP/SOFTWARE
 Configuration Control
 Procedure
Executive Order 11246
Existing security measures
Export Admin Regs
FAA DRAFT ORDER 1600
FAS Microcomputer Policy --
 Title 12 FASR, Ch.5
FBI Microcomputer Security
 Policy
FCC Rules and Regs
FDA 514.11 Confidentality of
 data/info in new animal
 drugs
FDA Staff Manual Guide
 2280.6
FED-STD 1027
Fed MANAGEMENT Fed INTEGRITY
 USE
FIFRA Confidential data
 handling procedures
FIPS PUBS 5,31,38,39,
 41,46,48,64,65,7
 3,77,81,83
FIPS PUBS 74,87,94,101,102,
 105,112,113,132
DOE/GSA Safety Reg.
EIA STD
FOE Safety and security
Fire Safety Code
FIRME section 2012-7.103-2
 (risk analysis guidance)
FIRMR
FMFIA/Internal Controls
FMP 311, ch. 732-735
FMS Security Policy Manual
Food, Drug and Cosmetic Act
Foreign Affairs Manual (FAM
 SECT 5, CHAPT 800 & 900)
FPM chapters
FPR 732
FPSO Configuration
 Management Plan D-4359
FRCP, Rule 6e, Grand Jury
 Secrecy of Proceedngs/Discl
Fair Credit Reporting Act
Fed Agency Responsblty for
 Maintn'g Records/Individuals
Fed Assistance Award Data
 System
Fed Credit Union Act of 1934 Fed
Government GAO Title II
 STD.
Fed Managers Financial
 Integrity Act
Fed Personnel Manual
Fed Property Mngt Regs
Fed Rules of Criminal
 Procedures 6(e)(1)
Fed security stds and
 approved industry
 procedures
Financial Management G/L
Financial Management Sys,
 Internal Control Sys
Financial Managers Integrity
 Act
Foreign Buildings Manual
 (FBO86)
Freedom of Info Act

OMB & Dept OIRM directives
GAAP
GAAS
GAO Accntg Sys Review &
 Audit Guides
GAO G/Ls
GAO Policy & Proc Manual for
 Guidance of Fed Agencies
GAO Principles and STD,
 Rules and Regs
GAO (Payroll) Title VI
GMI 2410.6A, ASSURING
 SECURITY/INTGRITY FOR GSFC
 DP
GSA Guidance to the Stand.
 Solic. Doc. for ADPE
GSA Regs & STD
GSA TSP Schedule
GSA Training Manual
GSA-DHHS Security Regs and
 G/LS
GSFC Computer Security Plan
Guide to Computer Protection
 at DOE
NASA G/LS for developing ADP
 risk reduction
Gen. Accounting Rules and
 Regs
Gen. Admin. Manual PHS
 Chapters 45-13
DOJ Guidance on Conducting
 Risk Analysis of ADP
 Facility
G/Ls developed by OMB, USDA
 & other Fed agencies
H-30-4, H-30-7
HCFA Admin issuance
 automatic data processing,
 sys sec polices
HCFA Admin Issuances System
 Guide
HHS STD of Conduct Regs
HP 9000 Manuals
HUD ADP STD & Documentation
 Manuals
HUD Handbook 2400.1 ADP
 Security Policy &
 Procedures
HUD IPS Documentation STDS
 Manual
HUD ADP Stds & Documentation
 Manuals
IAW FIPS PUBS
IBM Manuals
IEEE 802.3
IG AUDITS
INTERNATIONAL MOU'S
IRM P 2100.5
IRS CODE (AS AMENDED) SECTS.
 6103(1)(11), 6103(P)(4), &
 6402(C)
ITAR
Immigration and
 Naturalization Act
Info Tech. Security Manual
National Finance Center
 provided guidance
Info Resources Management
 Manual
InteCom and VMX Manuals
Internal Control Review
Directive
Internal Management Decision
JANAP 128, Fed Personnel
 Manual 732
JDC - Congressional mandate

executed by JDC
JPL Computer & Network
 Security G/LS/Handbook
JPL SPI 4-19
JPL Software Management Std
 D-4000
JSC AIS Handbook & AIS
 Security Plan
JSC AISSP
JSC Equipment Management
 Manual
JSCM 1600C Security Manual
KMI 2410.4A
LIMS Acceptance Test Plan
LIMS RFP
LMI 2410.3A & LMI 2410.9
LOCAL REGS FOR BUILDING
Low Observables Security
 Classification Guide
M204 STD
MANUAL OF OPS & ADMIN (MOA
 SECT 2, CHAPT 900)
MASS Program Devel Plan
 D-5179
MCCC Devel Section Standard
 Practice D 1816-15
Mission OPS & Data Sys
 Directorate Sys Mgmt Policy
 Document
MMI 2410.6
MP-6
MSFC FORM 2683 OCT. 1982
MSFC Source Evaluation Board
 Guide
Management of Fed Info
 Resources
Memo 1/12/87 from AAAG for
 Admin. Re Natl. Policy on
 Protection
Mission Operations CompuSec
 Training
Model Framework for Mgt.
 Control over AIS
NAS10-10600, S.W.O., W.B.B.S
 1.4.1, BOC STD & Procedures
NASA ADP Risk Analysis
 G/L/NASA Comm Div Sec Proc
 Manual
NASA AIS Program Handbook
NASA Financial Management
 Manual
NASA G/LS for certifying
 sensitive applications
NASA G/LS for contingency
 planning
NASA Handbook 1620.3B.
NASA Info Resource Handbook
 2410.1D
NASA JSC protection data
 laws and regulations
NASA Management instruction
 2410.7a
NASA MMI 2520.2
NASA G/Ls for meeting DOD
 Accreditation
NAT Policy on Telecom & AIS
 Security 9/17/84
NAT'AL Telecom & Info Sys
 Security Policy (NTISSP)-200
NBS SPEC PUB
 500-134, 500-120, 500-109,
 500-85
NCES STD Manual
NCHS Staff Manual on
 confidentiality
NCHS/TRP ADP Security Manual

NCIC Operating Manual
NCSC #WA-002-85, NCSC TG-005
NCSC Pubs
NCSC TCSE Criteria
NCSC TCSK Criteria
NCUA Standard Operations
 Procedure
NCUA/OIS Operating plans
NDPD Operational Policies
 Manual
NEA Internal Control
 Directive 1220, 1800
NEA Personnel Directives
NFPA 101
NHB 1610.6A, 2200.2, 2410.1
NHB 1620 "Physical Security
 Handbook"
NIH Data Center User's Guide NIH
 Requirements
NIH Standard Risk Protocol
NIST/NSA/OMB/DOC Guidance
NLA
NMI 2410.7A
NRC Appendix 2301, 2101
NRC Bulletin 2101-23
NRC Regulation 10 CFR
NRS & DOE RIGHTS
NSDD-145
NTIS ADP STD Manual
NTIS Info. Technology
 Security Manual
NTIS Methology for
 Certifying Sensitive
 Computer Applications
NTISSP's
Nat'al Info Systems Project
Nat'al Policy on
 Telecommunications and AIS
 Security
Nat'al STD for Arts Info
 Exchange
Nat'al level agency
 documents
No specific standards were
 used
None Listed
OASD Admin Instruction No.
 81
OASD Memorandum
OCC Info Systems Security
 Manual
OCIS Plans for classes,
 seminars and briefings
Off. of Solid Waste &
 Emergency Response Life Cycle
Guidance
OMB Circular A-123, A-130,
 A-127, A-129, A-13, A-124
OMB Bulletin 88-16
OMB Funds Control
 Requirements
OPP Sustem Devel Guidance
OPS Procedure
OSD Admin Instruction 26
OSWER Life Cycle Guidance
 1988
OMB Rules and Regs
Omnibus Diplomatic Security
 and Anti-Terrorism Act of
 1986
Operations STD and
 Procedures
PART 6, DHHS IRM Manual
PCIE Prevention Committee
PCMI/PCIE
PL 100-235 & PL 83-703

PSM 4-88, 5-88, 6-88
Policy & G/Ls Circular
 10-88-78
Privacy Act
Protective Order (Rule
 26(c))
Provided by Agr. Research
 Service LAN Manager and the
 ARS
Public Health Service Act
RACF Security STD
REE CO
RP-9-86 Course
RRB Board Order 75-2
RRB Data Processings STD and
 Procedures
Railroad Retirement Board
 (RRB) Vulnerability
 Assessment
Recovery Actions Plan
Reew Safety and Security
Regulation 1 of Social
 Security Admininstration
Relevant Fed STD
Rule 6, Fed Rules of
 Criminal Procedure
SAAS
SAIL Secure Ops Procedures
 Handbook
SBA SOP 90 47
SDI Contingency Plan
SDM70
SFIPEP Functional Reqirements
SIT Security Guide and Quality
 Assance
SSA's Regulation 1
STD industry practices
STS Program Security Mgmt
 Supplimental Agreement
 NASA/USAF
Section 331-338 of the PHS
 Act (42 U.S.C. 254 d-k)
Sections 301, 321 of Public
 Health Service Act (42 USC
 241, 248)
Sections 320, 321, 326 PHS
 Act, (42 USC 255,248,253)
Secure Environment
 Operator's Handbook
Security Management Plan
Shuttle Simulations Operations
 Handbook
Social Security Act
Specs for Contract between
 NASA ansd SCB/AS (NO.
 13-280)
Std Practice for the Fire
 Protection of Essential
Electronic Std security
 measures utilized by Off of
 Assist Attorn
Statement of Work in
 Contract NAS10-10600.
System Devel Methodology 70
 (SDM/70)
Treasure Directives 81-04,
 81-06, 83-01, 84-01, 84-02,
 85-01
Treasure Directives 35-02,
 85-0, 85-02, 85-03, 85-04
TFMIP
Title 18, USC, 1905
Treasury Financial Manual &
 Treasury Fiscal Manual
Tymnet Technical and User
 Manuals

Dept. of Interior Rules and
 Regs
U.S. Marshals Service Manual
UL STD
USCG Telecom Manual
USDA ADP Sec Manual (DM
 3140-1)
USDA Microcomputer Policy
 (DR 3130-1) & (DR 3130-2)
USDA's NFC G/Ls
USIA Manual of OPS and Admin
 (MOA SEC 2,CHAP 900)
USIA Security STDS for
 unclassified AIS
USM manual
Unknown
VA ADP Security Handbooks
 and Policies
VA ADP Security guidance
VA Manuals
VA Systems Devel Methodology VA
and Fed Regulation
VA-3001
VA-MP-6
Vendor Document recommendations
Vendor guidance
Vietnam   Era   Veterans
Readjustment Assistance Act
 of 1974
WANG Manuals & informal
 standards
Witness Security Division
 Internal Security G/Ls
bulletins, manuals,
 newsletters, and other
 policy issuances
in-house guidance & policies
independent contractor
 recommendations
operate the protective
 measures used on the system
other relevant documents
ss control lists at database
 and file levels

ABBREVIATIONS

G/L - Guidline
Dept - Department
Nat'al - National
Fed - Federal
Ops - Operations
CompuSec - Computer Security
Pgms - Programs
Devel - Development
Ed - Education
Admin - Administration
Sys -System

APPENDIX I

REFERENCES

PART I: GOVERNMENTWIDE APPLICABLE REFERENCES

The following is a list of documents that have government-wide applicability and/or are produced by organizations that have government-wide responsibility or jurisdiction.

CONGRESS

The Privacy Act of 1974 (Public Law 93-579)

The Freedom of Information Act of 1974 (Public Law 89-487)

The Paperwork Reduction Act of 1980 (Public Law 96-511)

The Federal Manager's Financial Integrity Act of 1982 (Public Law 97-255)

The Counterfeit Access Device and Computer Fraud Act of 1984 (Public Law 98-473)

The Computer Fraud and Abuse Act of 1986 (Public Law 97-474)

Computer Security Act of 1987 (Public Law 100-235) Plus background notes

GENERAL ACCOUNTING OFFICE

GAO/AFMD-86-14
Financial Integrity Act: The Government Faces Serious Internal Control and Accounting Systems Problems
December 1985

GAO/IMTEC-86-10
Contingency Plans and Risk Analyses Needed for IRS Computer Centers
March 1986

GAO/IMTEC-88-11
Information Systems: Agencies Overlook Security Controls During
Development
May 1988

GAO/IMTEC-86-11S
Appendix I Information Systems: Agencies Overlook Security
Controls During Development. "Model of Security in the System Life
Cycle Development Process"
May 1988

GAO/IMTEC-88-61BR
Computer Security: Status of Compliance with the Computer Security
Act of 1987
September 1988

GAO/T-88-8
Status of Compliance with the Computer Security Act of 1987
September 1988

GAO/IMTEC-89-16BR
Computer Security: Compliance with Training Requirements of the
Computer Security Act
February 1989

GAO/T-89-1
Status of Compliance with the Computer Security Act of 1987
March 1989

GAO/IMTEC-89-55
Computer Security: Compliance with Security Plans Requirements of
the Computer Security Act
June 1989

GAO/IMTEC-89-70
Computer Security: Identification of Sensitive Systems Operated on
Behalf of Ten Agencies
September 1989

GENERAL SERVICES ADMINISTRATION

"Information Security Oversight Office Directive No. 1 Concerning
National Security Information"
Security Oversight Office, (The Federal Register),
October 1978
Amendment to Federal Property Management Regulations Part 101-35
to add 101.35.3, "Security of Federal ADP and Telecommunications
Systems,"
(The Federal Register),
August 1980

(The Federal Register),
August 1980

Amendment to Federal Property Management Regulations Subpart 101-36.7, retitled "Environmental and Physical Security,"
(The Federal Register),
August 1980

Amendment to Federal Procurement Regulations to Section 1-4.1104, "Request for Procurement Action," (The Federal Register),
October 1980

Amendment to Federal Procurement Regulations to add Section 1-4.1107-21, "Computer Security Requirements,"
(The Federal Register),
October 1980

NATIONAL COMPUTER SECURITY CENTER

CSC-STD-002-85
Department of Defense Password Management Guideline
April 1985

CSC-STD-003-85
Computer Security Requirements. Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments
June 1985

CSC-STD-004-85
Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements. Guidance for Applying the Department of Defense Trusted Computer System
Evaluation Criteria in Specific Environments
June 1985

CSC-STD-005-85
Department of Defense, Magnetic Remanence Security Guideline
November 1985

DoD 5200.28-STD
Department of Defense Standard Department of Defense Trusted Computer System Evaluation Criteria (The Orange Book)
December 1985

NCSC-TG-001
Version-2A: Guide to Understanding AUDIT in Trusted Systems
June 1988

NCSC-TG-003

Version-1A: Guide to Understanding Discretionary Access Control
in Trusted Systems
September 1987

NCSC-TG-004,
Version-1: Glossary
October 1988

NCSC-TG-005
Version-1: Trusted NETWORK Interpretation
July 1987

NCSC-TG-006
Version-1A: Guide to Understanding Configuration Management in
Trusted Systems
March 1988

NCSC-TG-007
Version-1A: Guide to Understanding Design Documentation in
Trusted Systems
October 1988

NCSC-WA-002-85
Personal Computer Security Considerations
December 1985

Product Evaluation Bulletins,
distributed by the National Computer Security Center

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

FIPS PUB 4-1
REPRESENTATION FOR CALENDAR DATE AND ORDINAL DATE FOR
INFORMATION INTERCHANGE
January 1988

FIPS PUB 11
DICTIONARY FOR INFORMATION PROCESSING,
FIPS PUB 11-1
September 1977

FIPS PUB 31
GUIDELINES FOR ADP PHYSICAL SECURITY AND RISK
MANAGEMENT
June 1974

FIPS PUB 38
GUIDELINES FOR DOCUMENTATION OF COMPUTER PROGRAMS AND
AUTOMATED DATA SYSTEMS

February 1976

FIPS PUB 39
GLOSSARY FOR COMPUTER SYSTEMS SECURITY
February 1974

FIPS PUB 41
COMPUTER SECURITY GUIDELINES FOR IMPLEMENTING THE
PRIVACY ACT OF 1974
May 1975

FIPS PUB 46-1
DATA ENCRYPTION STANDARD
January 1988 (Reaffirmed until 1992)

FIPS PUB 48
GUIDELINES ON EVALUATION OF TECHNIQUES FOR
AUTOMATED PERSONAL IDENTIFICATION
April 1977

FIPS PUB 64
GUIDELINES FOR DOCUMENTATION OF COMPUTER PROGRAMS AND
AUTOMATED DATA SYSTEMS FOR THE INITIATION PHASE
August 1979

FIPS PUB 65
GUIDELINE FOR AUTOMATIC DATA PROCESSING RISK
ANALYSIS
August 1979

FIPS PUB 73
GUIDELINES FOR SECURITY OF COMPUTER APPLICATIONS
June 1980

FIPS PUB 74
GUIDELINES FOR IMPLEMENTING AND USING THE NBS DATA
ENCRYPTION STANDARD
April 1981

FIPS PUB 81
DES MODES OF OPERATION
December 1980

FIPS PUB 83
GUIDELINE ON USER AUTHENTICATION TECHNIQUES FOR
COMPUTER NETWORK ACCESS CONTROL
September 1980

FIPS PUB 87
GUIDELINES FOR ADP CONTINGENCY PLANNING

March 1981

FIPS PUB 88
GUIDELINE ON INTEGRITY ASSURANCE AND CONTROL IN
DATABASE APPLICATIONS
August 1981

FIPS PUB 94
GUIDELINE ON ELECTRICAL POWER FOR ADP INSTALLATIONS
September 1982

FIPS PUB 99
GUIDELINE: A FRAMEWORK FOR THE EVALUATION AND COMPARISON OF
SOFTWARE DEVELOPMENT TOOLS
March 1983

FIPS PUB 101
GUIDELINE FOR LIFECYCLE VALIDATION, VERIFICATION, AND TESTING
OF COMPUTER SOFTWARE
June 1983

FIPS PUB 102
GUIDELINE FOR COMPUTER SECURITY CERTIFICATION AND
ACCREDITATION
September 1983

FIPS PUB 105
GUIDELINE FOR SOFTWARE DOCUMENTATION MANAGEMENT
June 1984

FIPS PUB 106
GUIDELINE ON SOFTWARE MAINTENANCE
June 1984

FIPS PUB 112
STANDARD ON PASSWORD USAGE
May 1985

FIPS PUB 113
STANDARD ON COMPUTER DATA AUTHENTICATION
May 1985

FIPS PUB 132
GUIDELINE FOR SOFTWARE VERIFICATION AND VALIDATION PLANS
November 1987

FIPS PUB 139
INTEROPERABILITY AND SECURITY REQUIREMENTS FOR USE OF THE DATA
ENCRYPTION STANDARD IN THE PHYSICAL LAYER OF DATA COMMUNICATIONS
August 1983

FIPS PUB 140
GENERAL SECURITY REQUIREMENTS FOR EQUIPMENT USING THE DATA
ENCRYPTION STANDARD
April 1982

FIPS PUB 141
INTEROPERABILITY AND SECURITY REQUIREMENTS FOR USE OF THE DATA
ENCRYPTION STANDARD WITH CCITT GROUP 3 FACSIMILE EQUIPMENT
April 1985

NBS SPEC PUB 500-19
AUDIT AND EVALUATION OF COMPUTER SECURITY
Zella G. Ruthberg, Robert G. McKenzie
October 1977

NBS SPEC PUB 500-20
VALIDATING THE CORRECTNESS OF HARDWARE IMPLEMENTATIONS OF THE NBS
DATA ENCRYPTION STANDARD
By Jason Gait
November 1977

NBS SPEC PUB 500-54
A KEY NOTARIZATION SYSTEM FOR COMPUTER NETWORKS
By Miles E. Smid
October 1979

NBS SPEC PUB 500-56
VALIDATION, VERIFICATION, AND TESTING FOR THE INDIVIDUAL
PROGRAMMER
By Martha A. Branstad, John C. Cherniavsky,
and W. Richards Adrion
February 1980

NBS SPEC PUB 500-57
AUDIT AND EVALUATION OF COMPUTER SECURITY II: SYSTEM
VULNERABILITIES AND CONTROLS
Zella Ruthberg, Editor
May 1980

NBS SPEC PUB 500-61
MAINTENANCE TESTING FOR THE DATA ENCRYPTION STANDARD
By Jason Gait
August 1980

NBS SPEC PUB 500-75
VALIDATION, VERIFICATION, AND TESTING OF COMPUTER SOFTWARE,
Adrion W. Richards, Martha A. Branstad, John C. Cherniavsky
April 1980

NBS SPEC PUB 500-85
EXECUTIVE GUIDE TO CONTINGENCY PLANNING

By James K. Shaw and Stuart W. Katzke
January 1982

NBS SPEC PUB 500-88
SOFTWARE DEVELOPMENT TOOLS
Raymond C. Houghton Jr.
March 1982

NBS SPEC PUB 500-93
SOFTWARE VALIDATION, VERIFICATION, AND TESTING TECHNIQUE AND TOOL
REFERENCE GUIDE
Patricia B. Powell, Editor
September 1982

NBS SPEC PUB 500-98
PLANNING FOR SOFTWARE VALIDATION, VERIFICATION, AND TESTING
Patricia B. Powell, Editor
November 1982

NBS SPEC PUB 109
OVERVIEW OF COMPUTER SECURITY CERTIFICATION AND ACCREDITATION
By Zella Ruthberg and William Neugent
April 1984

NBS SPEC PUB 500-120
SECURITY OF PERSONAL COMPUTER SYSTEMS: A MANAGEMENT GUIDE
By Dennis D. Steinauer
January 1985

NBS SPEC PUB 500-133
TECHNOLOGY ASSESSMENT: METHODS FOR MEASURING THE LEVEL OF
COMPUTER SECURITY
By William Neugent, John Gilligan, Lance Hoffman, and
Zella G. Ruthberg
October 1985

NBS SPEC PUB 500-134
GUIDE ON SELECTING ADP BACKUP PROCESSING ALTERNATIVES
By Irene E. Isaac
November 1985

NBS SPEC PUB 500-136
AN OVERVIEW OF COMPUTER SOFTWARE ACCEPTANCE TESTING
By Dolores Wallace
February 1986

NBS SPEC PUB 500-137
SECURITY FOR DIAL-UP LINES
By Eugene F. Troy
May 1986

NBS SPEC PUB 500-153
GUIDE TO AUDITING FOR CONTROLS AND SECURITY: A SYSTEM
DEVELOPMENT LIFE CYCLE APPROACH
Editors/Authors: Zella G. Ruthberg, Bonnie T. Fisher, William E.
Perry, John W. Lainhart IV, James G. Cox, Mark Gillen, and
Douglas B. Hunt
April 1988

NBS SPEC PUB 500-156
MESSAGE AUTHENTICATION CODE (MAC) VALIDATION SYSTEM:
REQUIREMENTS AND PROCEDURES
By Miles Smid, Elaine Barker, David Balenson and Martha Haykin
May 1988

NIST SPEC PUB 500-157
SMART CARD TECHNOLOGY: NEW METHODS FOR COMPUTER ACCESS CONTROL
By Martha E. Haykin and Robert B. J. Warnar
September 1988

NBS SPEC PUB 500-158
ACCURACY, INTEGRITY, AND SECURITY IN COMPUTERIZED VOTE-TALLYING
By Roy G. Saltman
August 1988

NIST SPEC PUB 500-160
REPORT OF THE INVITATIONAL WORKSHOP ON INTEGRITY POLICY IN
COMPUTER INFORMATION SYSTEMS (WIPCIS)
Stuart W. Katzke and Zella G. Ruthberg, Editors
January 1989

NIST SPEC PUB 500-163
GOVERNMENT OPEN SYSTEMS INTERCONNECTION PROFILE USERS' GUIDE
By Tim Boland
August 1989

NIST SPEC PUB 500-165
SOFTWARE VERIFICATION AND VALIDATION: ITS ROLE IN COMPUTER
ASSURANCE AND ITS RELATIONSHIP WITH SOFTWARE PROJECT MANAGEMENT
STANDARDS
By Dolores R. Wallace and Roger U. Fujii
September 1989

NIST SPEC PUB 500-166
COMPUTER VIRUSES AND RELATED THREATS: A MANAGEMENT GUIDE
By John P. Wack and Lisa J. Carnahan
August 1989

NIST SPEC PUB 500-167
INFORMATION MANAGEMENT DIRECTIONS: THE INTEGRATION CHALLENGE
Elizabeth N. Fong and Alan H. Goldfine, Editors
September 1989

NIST SPEC PUB 500-168
REPORT OF THE INVITATIONAL WORKSHOP ON DATA INTEGRITY
By Zella G. Ruthberg and William T. Polk
September 1989

NIST SPEC PUB 500-169
EXECUTIVE GUIDE TO THE PROTECTION OF INFORMATION RESOURCES
October 1989

NIST SPEC PUB 500-170
MANAGEMENT GUIDE TO THE PROTECTION OF INFORMATION RESOURCES
October 1989

NIST SPEC PUB 500-171
COMPUTER USER'S GUIDE TO THE PROTECTION OF INFORMATION RESOURCES
October 1989

NIST SPEC PUB 500-172
COMPUTER SECURITY TRAINING GUIDELINES
November 1989

NIST SPEC PUB 500-174
GUIDE FOR SELECTING AUTOMATED RISK ANALYSIS TOOLS
October 1989

NBSTIR 86-3386
WORK PRIORITY SCHEME FOR EDP AUDIT AND COMPUTER SECURITY REVIEW
By Zella Ruthberg and Bonnie Fisher
August 1986

NBSIR 88-3700 (supersedes NBSIR 85-3164)
A TECHNICAL OVERVIEW OF THE INFORMATION RESOURCE DICTIONARY
SYSTEM (Second Edition)
By Alan Goldfine and Patricia Konig
January 1988

NBSIR 88-3701 (supersedes NBSIR 85-3165)
USING THE INFORMATION RESOURCE DICTIONARY SYSTEM COMMAND LANGUAGE
(Second Edition)
By Alan Goldfine
January 1988

NISTIR 89-4053
ARCHITECTURALLY FOCUSED BENCHMARKS WITH A COMMUNICATION EXAMPLE
By G.E. Lyon and R.D. Snelick
March 1989

NISTIR 89-4128
PROCESSING RATE SENSITIVITIES OF A HETEROGENEOUS MULTIPROCESSOR
By Gordon Lyon
August 1989

NISTIR 89-4140
WORKING IMPLEMENTATION AGREEMENTS FOR OPEN SYSTEM INTERCONNECTION
PROTOCOLS
Tim Boland, Editor
September 1989

NISTIR 89-4160
TRIAL OF OPEN SYSTEMS INTERCONNECTION (OSI) PROTOCOLS OVER
INTEGRATED SERVICES DIGITAL NETWORK (ISDN)
by Carol A. Edgar
August 1989

NIST PUBLICATIONS LIST 91
Computer Security Publications
March 1990

OFFICE OF MANAGEMENT AND BUDGET

OMB Circular A-123,

11

"Internal Control Systems"
October 1981
Questions and Answers on Circular A-123 (Revised),
"Internal Control Systems"
August 1984

OMB Circular A-130,
"Management of Federal Information Resources"
December 1985

OMB Bulletin No. 88-16,
"Guidance for Preparation and Submission of Security
Plans for Federal Computer Systems Containing Sensitive
Information
July 1988

OFFICE OF PERSONNEL MANAGEMENT

Federal Personnel Manual 731 and 732,
"Personnel Screening"
January 1984.

PART II: AGENCY-SPECIFIC REFERENCES

The following list of agency-specific references is NOT COMPLETE. It is presented as a sampling of policy and guidance documents published by individual agencies.

DEPARTMENT OF AGRICULTURE

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

"ADP Security Handbook,"
USDA DIPS Manual Supplement

DEPARTMENT OF DEFENSE

Air Force Regulation 205-16,
"Computer Security Policy"

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"

Army Regulation 380-380,
Automation Security
March 1987

Assistant Secretary of Defense Comptroller Memorandum,
"Interim Policy on Safeguarding Personal Information in ADP Systems"

DoD Directive 5200.28,
"Security' Requirements for Automatic Data Processing (ADP) Systems"

DoD Manual 5200.28-M,
"ADP Security Manual Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource Sharing ADP Systems"

NSA/CSS Directive 10-27,
"Security Requirements for Automatic Data Processing (ADP) Systems"

NSDD-145
NTISSP No. 200
Scowcroft Memo
OMB and NSA NSDD-145 rewrites
The Warner Amendment

OPNAVISNT 5239.1,
"Department of the Navy Security Program for Automatic Data
Processing Systems"

OPNAVINST 5239.1A,
"Department of the Navy ADP Security Manual"

DEPARTMENT OF ENERGY

DOE Order 1360.2,
"Computer Security Program for Unclassified Computer Systems"

DOE Order 5635.2,
"Security' Requirements for Classified Automatic Data Processing Systems"

DOE Manual 5636.2,
"Computer Security Guidelines for Classified Automatic Data Processing Systems"

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Part 6,
"ADP Systems Security," Chapter 6,
HHS ADP Systems Manual

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

"HUD ADP Security Policy Handbook"

DEPARTMENT OF THE INTERIOR

306 DM 7,
Departmental Management Part 306 (Automatic Data Processing),
Chapter 7
(ADP Security Program)

"ADP Standards Handbook" (306 DM), Chapter 2 (ADP Security Program)

DEPARTMENT OF JUSTICE

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

Basic Considerations in Investigating and Proving
Computer-Related Federal Crimes
November 1988

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 THE TREASURY

DOT Order 102-3,
"Personnel, Physical and Automatic Data Processing (ADP) Systems
Security-Organization and Delegation of Authority"

Treasury Directive 1008, Part VII,
"ADP Resource Protection"

Treasury Directive 1008, Part Va
"ADP Privacy Act Guidelines"

Treasury Directive 1008, Part VII, (DRAFT)
"ADP Resource Protection Guidelines"

FEDERAL AVIATION ADMINISTRATION

"Security Certification Guidelines for the Federal Aviation
Administration's Uniform Payroll System"

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

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

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

PART III: MISCELLANEOUS PUBLICATIONS

PRESIDENT'S COUNCIL ON INTEGRITY AND EFFICIENCY (PCIE)

Model Framework for Management Control Over Automated Information
System
January 1988

Review of General Controls in Federal Computer Systems
October 1988

IBM

The Considerations of Physical Security in a Computer Environment
October 1972

Information Security Program Manager's Guide
February 1985

Security Risk Assessment in Electronic Data Processing Systems
January 1984

MVS Security
March 1984

Good Security Practices for Dial-Up Systems
March 1984

Good Security Practices for Personal Computers
March 1984

Security, Auditability, System Control Publications Bibliography
May 1985

Information Systems Security Controls and Procedures
February 1986

Good Security Practices for Information Systems Networks
March 1987

Contingency Planning for Catastrophic Events in Data Processing
Centers
September 1981

Good Security Practices for Control of Off-Site Terminal and
Software Usage
December 1984
IBM Information Network Security Bulletin
July 1985

Communications Systems Bulletin, An Executive Overview of
Information Network Management
May 1986

OTHER

Final Report of the Industry Information Security (IIS) Task
Force

Industry Information Protection, Volume II.   Appendices
June 1988

Industry Information Protection, Volume III.   Annotated
Bibliography
June 1988

"Plan Evaluation Guide," Computer Security Plan Review Project
January 1989

APPENDIX J

EXAMPLES OF AGENCY REACTIONS TO CSPP REVIEWS

September 28, 1989

Computer Security Plan Review Team
National Institute of Standards
     and Technology
Gaithersburg, Maryland   208099

Dear Sirs:

     The Consumer Product Safety Commission staff has reviewed
the comments of the NIST review team on our Computer Security and
Privacy Plans. The review team noted some weaknesses. We have
looked carefully at these areas and find that the apparent lack
of coverage was the result of staff misinterpretation of the
guidelines for preparing the plans. The requisite procedures and
controls, including a comprehensive ADP security directive, were
in fact in place. Further, our ADP security directive, which was
not referred to in the plans, covers most of the purposes of the
optional agency overview suggested by the review team.

     We appreciate the careful review our plans received. I
have asked the staff to bring them up to date and to address the
areas pointed out by the review team so that the plans will
contain statements of all the appropriate procedures and
controls.

                         Sincerely,

                         Thomas W. Murr, Jr.
                         Acting Executive Director

Douglas B. Hunt and Christopher P. Bythewood
Managers, Computer Security Plan Review Team
National Institute of Science and Technology (NIST)
Technology Building
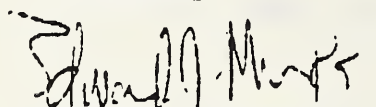Gaithersburg, Maryland 20899

Dear Messrs:

The Federal Communications Commission is very appreciative of the comments
made by the Review Team concerning this agency's submission of Computer
Security and Privacy Plans (CSPPs). Your timely and thought provoking remarks
have been extremely helpful in our refinement of our original submission.
We have addressed, improved, or corrected each issue that was raised. Allow
me, however, to just reiterate several major issues that you brought to our
attention:

o Due to a reallocation of existing resources, the agency was able
   to successfully recruit and select a Program Analyst for the Computer
   Security Program during FY 89 instead of FY 90 as originally projected.

o Based upon your remarks concerning the unique security requirements of
   the agency's LAN, we have requested the purchase of a Gateway computer
   from the FY 91 budget. This should provide the necessary security
   controls for the network environment.

o The FCC's Security Awareness Training program, originally implemented in
   FY 88 and still ongoing, is designed to provide different levels of
   training to the diverse group of users here at the agency. This program
   involves every employee, manager, supervisor and executive involved in
   the use of the agency's sensitive systems. This training program will
   continue with classes for new employees and special briefings as new
   issues are confronted.

o The agency currently has a personnel selection/screening program in place
   (FCCINST 1120.1A), administered by the Internal Control and Safety
   Office. As no additional program is required, we are already in
   compliance with OMB Circular A-130 and have annotated the plans
   accordingly.

o The agency, in conjunction with the Navy Regional Data Automation Center (NARDAC), did complete a formal risk assessment program. The combination of a Los Almos National Laboratory Vulnerability Assessment (LAVA) study and our own internal computer security survey meet the formal requirements of FIPS Pub. 64, Factor II. These entries have also been corrected on the CSPPs.

Again, allow me to express our gratitude for the guidance and assistance your comments and suggestions have provided.

Sincerely,

Edward J. Minkel
Managing Director

cc: Mr. Frank Reeder, OMB

Dr. Stuart W. Katzke
Mr. Christopher P. Bythewood
The Computer Security Plan Review Team
The National Institute of Standards and Technology
Technology Building
Gaithersburg, MD. 20899

Dear Dr. Katzke and Mr. Bythewood:

The Environmental Protection Agency (EPA) has reviewed the
Computer Security Plan Review Team's analysis and recommendations
for the Agency's computer security plans. The purpose of this
letter is to share with you the Agency's plans for addressing the
concerns and comments of the Review Team.

EPA received its security plans back from the Review Team in
late September. In the near future, the Office of Information
Resources Management (OIRM) will be forwarding the
recommendations and analysis regarding each individual plan to
the responsible system manager/security officer and to the
responsible Senior IRM Official for review and action. (EPA
maintains a network of 21 Senior IRM Officials, one for each
major program and administrative function and one for each of the
10 regions.) Within six months, OIRM will solicit a written
status report from each plan preparer concerning actions taken in
response to the Review Team comments. If insufficient action has
been taken, OIRM will schedule a meeting with the cognizant
Senior IRM Official to identify needed steps.

The Review Team highlighted two areas that may require
attention. The first area involves the certification/accreditation
of sensitive systems. The EPA security planning process indicated:
(1) that systems typically met applicable policies, regulations,
and standards, and (2) that system security controls were tested
before the system became operational. In a number of instances,
however, a formal "sign off" process for the security controls by
a certifying or accrediting official did not take place.

EPA has identified this certification/accreditation weakness as an Agencywide security priority in its recent OMB Bulletin No. 89-17 response. As an important step in addressing this weakness, EPA has developed final versions of two security manuals, one exclusively for PCs and one dealing comprehensively with all types of information assets. Both manuals include procedures for certification/accreditation, including a form for formal authorization of a system.
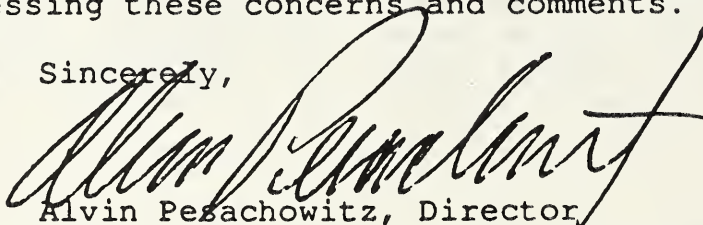
The second area of concern highlighted by the Review Team was related to inadequate descriptions of system sensitivity in a number of the plans. OIRM believes that this area of concern reflects our misinterpretation of the level of detail required by OMB Bulletin No. 88-16 more than it reflects a substantive weakness. In putting information into a standard format to respond conscientiously to 88-16 requirements, the Agency made judgments about the level of detail to supply.

As noted in the descriptive documentation that EPA submitted along with its plans, each plan represented a fresh undertaking because in no instance was there an existing document that would fully satisfy the OMB 88-16 requirements. In the case of the "General Description of Information Sensitivity" section, the Agency did not always supply information about how the relationships among system functions, system environment, and the nature of the information created vulnerabilities and the need for protective measures. Clearly, an important aspect of safeguard selection involves recognizing the threats to a system and understanding the consequences if those threats are realized. These factors are emphasized in the two security manuals, and future security plans will provide more detailed explanation in this area.

The Review Team's summary analysis also commented on two other areas: (1) security awareness and training, and (2) risk analysis. The Agency has obtained the referenced "Computer Security Training Guidelines" and is using them as it expands its training/awareness program. Also, each security manual now includes a separate appendix on risk analysis methodology.

The Review Team clearly performed a detailed analysis of our plans. I appreciate this opportunity to share with you the Agency's plans for addressing these concerns and comments.

Sincerely,

Alvin Pesachowitz, Director
Office of Information Resources Management

cc: Edward J. Hanley

NIST-114A (REV. 3-90)	U.S. DEPARTMENT OF COMMERCE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY	1. PUBLICATION OR REPORT NUMBER NISTIR 4409
		2. PERFORMING ORGANIZATION REPORT NUMBER
BIBLIOGRAPHIC DATA SHEET		3. PUBLICATION DATE September 1990

4. TITLE AND SUBTITLE

1989 Computer Security and Privacy Plans (CSPP) Review Project: A First-Year Federal Response To The Computer Security Act of 1987 (Final Report)

5. AUTHOR(S)

Dennis M. Gilbert

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

Department of Defense
National Computer Sec. Ctr
9800 Savage Road
Ft. George G. Meade, MD

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED

FINAL

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)

10. SUPPLEMENTARY NOTES

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

The goal of the Computer Security Act of 1987 (Public Law 100-235) (the Act) is to prompt federal agencies to take measures to improve the security and privacy of sensitive information in federal computer systems. The Act requires federal agencies to prepare and submit for review security plans for all computer systems that contain sensitive information. The Act provides that the plans be submitted to the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) for review and comment. This report describes the Computer Security and Privacy Plan (CSPP) review effort that was conducted in response to the Act by a joint team from NIST and NSA in 1989. The report also discusses future directions for implementing the Act.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

Computer Security Act; guidance; unclassified sensitive information

13. AVAILABILITY

X	UNLIMITED
	FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).
	ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.
X	ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES

189

15. PRICE

A09

ELECTRONIC FORM

IR 4410

NEVER PUBLISHED