NISTIR 5424

A Study of Federal Agency Needs for Information Technology Security

Dennis M. Gilbert

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Computer Security Division
Computer Systems Laboratory
Gaithersburg, MD 20899

NIST

NISTIR 5424

A Study of Federal Agency Needs for Information Technology Security

Dennis M. Gilbert

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Computer Security Division
Computer Systems Laboratory
Gaithersburg, MD 20899

May 1994

U.S. DEPARTMENT OF COMMERCE
Ronald H. Brown, Secretary

TECHNOLOGY ADMINISTRATION
Mary L. Good, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arati Prabhakar, Director

PREFACE

This (draft) report presents the results of a NIST study to determine and document what federal agencies need to meet their information technology (IT) security requirements. A meeting of the NIST IT Security Needs Study Working Group was held at NIST in September 1992 to review and comment on the study results. This report reflects the working group input.

It should be noted that this study was conducted before such subjects as the National Information Infrastructure (NII) and the information super highway had reached the levels of public awareness and discussion that they currently enjoy. However, a rapidly changing technological environment was an implicit assumption of the study. It is felt that the study results are still relevant, appropriate, and timely.

ABSTRACT

In carrying out its charter to help federal agencies meet their individual information technology (IT) security requirements, the National Institute of Standards and Technology (NIST) must understand what agencies need to meet those requirements. The initial effort to improve NIST's ability to identify and assess these agency needs consisted of reviewing existing documented sources of IT security-related requirements and needs, conducting an in-depth study, and establishing ongoing mechanisms to facilitate communication between NIST and agencies. The recently conducted study involved interviews with federal agency staff and a survey in which respondents indicated the importance and immediacy of a set of three dozen candidate needs. Study participants were selected to represent a wide variety of federal IT security environments, applications, individual perspectives, and data processing environments.

The results of the study contribute to a sound basis for planning future NIST IT security standards, guidance, and related activities. NIST is committed to developing and documenting a clear understanding of agency needs in this area and to using the documented, validated needs as input to its program planning process.

This report documents the study.

EXECUTIVE SUMMARY

INTRODUCTION

NIST has completed a study to help understand and document what federal agencies need to satisfy their information technology (IT) security requirements. NIST will consider the study results in shaping its programs to help agencies satisfy those needs and to plan for the effective use of NIST resources. In addition to NIST IT security management, other potential audiences of this report include those agency staff concerned with IT security management, policy, planning, implementation, and training. The report can be used by these staff to consider their IT security needs or provide input to those who may be a source of help. (Note: For the remainder of this Executive Summary, the term *"security"* refers to *"IT security."*)

The study, conducted from February to August 1992, focused on five **target agencies**, selected to represent a variety of federal security environments. These agencies were the Department of Commerce, Department of Education, Department of Justice, National Aeronautics and Space Administration, and Social Security Administration. The study involved interviews with agency staff and the use of an IT security needs assessment survey. Respondents were asked to identify their security needs from a list of three dozen candidates and indicate the importance (*none*, *low*, *medium*, *high*, and *very high*) and immediacy (*immediate*, *near term*, and *long term*) of each. Other federal, private sector, and professional organizations were invited to participate.

Security needs data were gathered from the target agencies. A dozen interviews were conducted with approximately 85 agency staff participating in the interviews. Survey responses numbered 224. Each **target agency representative (TAR)**, the prime contact from each target agency, identified those in his/her organization to be interviewed and to receive surveys. This was done following discussion among the **study team**, which consisted of the TARs and the NIST study coordinator. (Note: The study team was sometimes augmented by NIST staff for the interviews.)

A **study working group**, consisting of approximately 30 invited federal and private sector representatives, provided direction to the study. The group met in February 1992 to comment on the overall approach and methodology, and again in September 1992 to review the study results. This study report reflects the working group input.

PROFILE OF SURVEY RESPONDENTS AND RESPONSES

Of the 224 total survey responses, 88 percent came from the target agencies. Two of the responses indicated they represented a single "corporate" reply for their agency. Of those respondents that indicated a government grade, 44 percent were GS or GM 13 or 14 and 24 percent were GS or GM 15 or SES. Twenty-eight percent indicated they were a computer security officer; 19 percent indicated computer, data processing (DP), or information resources management (IRM); and 9 percent indicated functional or line management. Thirty-three percent reported less than one year security-related experience and 19 percent reported three to five years of such experience. Almost half (47 percent) chose not to provide this information. Survey respondents were provided the opportunity to request anonymity and approximately 40 percent chose to do so.

RESPONDENT RATINGS OF SURVEY CANDIDATE NEEDS

The 36 candidate needs from the survey were organized and presented to respondents in four groups. Respondents rated both the importance and immediacy of each candidate need. Ratings were converted to numbers. Based on these numbers, "weighted" average importance and immediacy values were calculated for each of the 36 candidate needs. However, because it appears respondents gave more attention to responses concerning importance than to those concerning immediacy, and because there was a strong relationship between importance and immediacy in survey responses, the rest of the analysis was based primarily on importance responses.

FINDINGS AND OBSERVATIONS

General

Some people are looking for the "silver bullet" for their security concerns, and, of course, there is none. The good news, however, is that there were very few of these people among those interviewed and much of the help requested in the interviews and survey responses already exists or is being developed by NIST and others. Also, many agencies are making a significant effort to identify and solve

their security problems.

Many security needs were expressed in the course of the study. Some were simple. Some were complicated. Some were tangential. Many were fundamental. Most were interrelated. The study team noted only 24 percent of the surveys expressed one or more additional needs and only 13 percent provided additional comments.

A number of those interviewed expressed appreciation at the opportunity to focus on security, and also to discuss their problems and frustrations. A number of people said they saw the survey as a tool they could use to better understand the security needs of their constituency.

Overall, needs related to technical approaches, methodologies, and products were rated higher in average importance than other subgroups of candidate needs. Needs in this group, in turn, consisted of a subgroup addressing "specific security environments" and a subgroup addressing "particular areas of concern." The security environments subgroup included needs related to *LANs*, *linking systems in one security architecture*, *integrating open system products*, *secure dial-in and laptops*, and *database security*. This subgroup provided the strongest showing as a subgroup.

The subgroup that addressed particular areas of concern included needs related to *access control and authentication*, *public access by client populations*, *individual user accountability*, *minimum controls for sensitivity levels*, *satisfying (inter)national criteria*, *troubleshooting security problems*, *security in software development and software engineering*, and *computer security tools evaluations*. This subgroup had the lowest average as a subgroup.

Findings and Observations

Below is a summary of the findings and observations made during the agency security needs study, expressed in terms of issues that emerge from the study. As may be expected, remarks made in the interviews and additional comments offered by survey respondents do not fall into neat, distinct categories. Overlaps and interrelationships exist. It is the opinion of the study team that some of the remarks made by study participants may be based on an incomplete or inaccurate understanding on the part of the respondents or interviewees, or the result of misinterpretations or miscommunications among study participants and

the study team. (See the full report for discussion of the issues listed below.)

Some General Issues

- Concern was expressed about dealing with new and changing technical and processing environments
- A more detailed understanding of security requirements is desired
- "Filtering" or simplifying of requirements is wanted by users less sophisticated about security issues and concerns
- Study participants see NIST as a key player in addressing their security needs

Issues Concerning Policy, Management, and Planning

- Many respondents feel hampered by limited resources and budgets and frustrated in justifying security resources
- Users want security requirements to be reasonable and relevant
- Users want realistic, practical, integrated federal security policy
- There were varying perspectives regarding the need for additional "external" security requirements, i.e., those placed by federal oversight organizations
- Security needs to be integrated into overall management and planning
- Users are concerned about addressing security in an environment of competing (production and other) demands
- Users are concerned about defining, identifying, and protecting sensitive information and systems
- Users want to know how to securely share/exchange data and resources with other agencies and with industry
- Users want to know how to address security throughout the system development life cycle
- Help is wanted in communicating with vendors and contractors

Issues Concerning Basic Security Functions and Activities

- Users want tools and guidance regarding risk management
- In protecting sensitive systems, users want to know what is expected, appropriate, and adequate

- Contingency planning, disaster recovery, and backups were identified as significant issues by survey respondents

Issues Concerning Security Awareness and Training

- There is strong support for security awareness and training
- Executive-level security awareness and training are viewed as critical to obtaining top management support

Issues Concerning Technical Approaches, Methodologies, and Products Dealing with Security

- Technical approaches to satisfy security objectives must be simple, cheap, practical, and "real world"
- Help is sorely needed in applying security in LANs, networks, and open systems, and to workstations and PCs in these environments
- Significant interest was expressed in security of databases, distributed data, and distributed processing
- There was some interest in products and tools to control access
- There was moderate interest in identification, authentication, and encryption and some confusion about alternatives
- Federal criteria, trusted products, and the need for technical evaluation of products rated low in the survey compared to other needs

Issues Concerning Security Information and Sources of Help

- There is lack of awareness of available sources of help
- A clearinghouse and the free flow of information about security are wanted

CONCLUSIONS

These conclusions are based on discussions among the study team, the TARs, the study working group, and NIST staff. The study working group, at a meeting in September 1992, indicated that the needs expressed in this report are consistent with the data presented and with their experience and understanding of the

federal security environment.

It should be noted that the study did not find security needs that were unimportant. It appeared to the study team that assistance in any of the need areas would be of value to at least some of the study participants. However, taken as a whole, some needs were clearly identified as more important to the participants than others. A full appreciation by study participants of all of the needs may have to wait for more universal and in-depth awareness and understanding of security issues and technology.

There is a Need for New NIST Technical Guidance Documents and for a Major Revision/Update of Existing Documents

The study team found a clear need for a major revision and update of a number of the NIST FIPS publications and related technical guidance documents, as well as the need for new documents. The following areas were explicitly identified in the survey (i.e., ranked among or near the top third) as requiring attention. Their importance to study participants was echoed in the interviews and affirmed by the study working group. (Respective importance rankings are given in parentheses.)

Specific technical environments needing attention:

- LANs (rank 1)
- the integration of PCs, LANs, and mainframes in one security architecture (rank 2)
- database security (rank 3)
- secure dial-in and laptops (rank 6)
- integration of open system environment products (rank 11)

Policy, management, and technical areas and basic security functions needing attention:

- security in the system development life cycle (rank 4)
- contingency and disaster recovery planning (rank 5)
- defining and protecting sensitive systems (rank 8)
- developing security plans (rank 9)
- risk analysis (rank 10)
- information collection, dissemination, and sharing (rank 12)

There is a Need to Help Agencies Develop Robust and Integrated Security Programs

It appears to the study team that agencies need help in developing robust and integrated security programs. Such a program is more than a collection of computer security and privacy plans prepared in accordance with Office of Management and Budget (OMB) Bulletin 90-08, but includes the full range of technical policies and procedures and the implementation of cost-effective, risk-based controls. It also includes federal policy integrating security, IRM, personnel, acquisition, internal controls, and financial management.

There is a Need for More Federal and Agency Security Resources, and a Need to Better Leverage Resources

A frequently heard theme during the study was that there were not enough security resources to do the job the way those who had direct responsibility for security would like to do it. This translates into a need for additional resources, a way to better leverage existing resources, or a combination of both.

There is a Need to Access Relevant Information and a Need to More Effectively Share Information

The study team and study working group found a strong need for a national state-of-the-art clearinghouse of all public domain security documents and publications, and a strong need to find more structured ways in which to facilitate cooperative efforts among agencies to share knowledge, experience, and documents developed by federal agencies. The study working group encouraged the use of special focused workgroups to collaboratively address the updates, revisions, and new documents, and they reported a willingness on the part of the federal security community to participate in such efforts. The study working group also saw potential value in establishing an electronic group decision support system (GDSS) center that could be used to more effectively facilitate group-developed guidance documents and training tools in the area of IT security.

There is a Need for Guidance and Assistance and for Authoritative Information Regarding Security

There was general agreement on the need for, and value of, guidance and

assistance in the technical and non-technical areas of security. There was also a related need for an "authoritative" source for information regarding security policy and the application of security technology.

There is a Lack of Consensus Regarding the Need for Stronger Federal and Agency Security Policy

Some study participants wanted to see both governmentwide and agencywide enforcement language and mechanisms to put "teeth" into security policy. There were others, however, that felt very strongly that establishing additional security requirements through federal directives was unnecessary and could be counter-productive.

There is a Need to Raise the Level of Security Awareness of Agency Management and Raise the Stature of Security Practitioners

Study participants were concerned about level of awareness of security issues by executives, functional managers, and information resource managers. It was felt that lack of awareness by these people made it extremely difficult to communicate with them about security and for security to effectively compete for resources with other management concerns. In many organizations, security continues to be an "additional duty." The study working group felt that establishing a separate job series for security professionals would raise management awareness about the importance of security. It was also felt that actions leading to the professionalization of security practitioners was a positive step.

There is a Need to Better Anticipate Security Requirements and Needs and Better Anticipate What Kinds and Forms of Support Will be Available

Agencies need to do a better job anticipating their security requirements and needs. Vendors would be better able to respond to changing government security repuirements, if these needs are more effectively communicated. This process could be helped if federal planners provided information about long range strategic directions. Also helpful would be stronger federal liaisons with the vendor community so the availability of vendor products will be "in sync" with near-term and long-term federal security needs.

IN SUMMARY

Those organizations the study team worked with and visited appear to have a deep commitment to security, despite a number of constraints, limitations, and frustrations. They are looking for a clear statement of what is required and expected of them with regard to security - and they expect these requirements to make sense and to be consistent with their other requirements.

While agencies regard NIST as one important source for help, they are by no means standing idly by. They are actively developing programs that work for them. They are also beginning to coordinate their efforts with other agencies. There is clearly a need for federal agencies to continue to be proactive regarding security and define the role they will assume in their own behalf. In this regard, it is recommended that federal agencies continue to monitor their security needs, communicate these needs to the central agencies, seek sources of help from within the federal community, and be generous in the sharing of their own experiences, efforts, and products.

Finally, this study is but one piece of a much larger mosaic. We believe this study is an important element in providing a sound basis for planning future NIST security-related efforts. In addition to NIST and the other central agencies, each agency's staff, including agency security, management, and individual users, are among those who play an integral role in providing comprehensive security for the federal government. In deciding where to apply resources and energies, it is important to take into account the roles and relationships among all these players. There is an open invitation and welcome for all to join in the search for and development of solutions that serve our community.

ACKNOWLEDGEMENTS

STUDY PARTICIPANTS AND REPORT CONTRIBUTORS

Dennis Gilbert, NIST Study Coordinator
Judy Bloom, DOJ, TAR
Lisa Carnahan, NIST
Rick Carr, NASA, TAR
Charles Dinkel, NIST
Jack Garnish, SSA, TAR
Bob Gignilliat, HHS, AC
Irene Gilbert Perry, NIST
Judy Gilsinn, NIST, AC
Marty Gray, NIST
Joan Hash, SSA, TAR
Barbara Guttman, NIST
D. Richard Kuhn, NSIT
Patrick Leone, PTO, AC
Nickilyn Lynch, NIST
Sadie Pitcher, DOC
Dennis Steinauer, NIST
Merv Stuckey, formerly Census, AC
Marianne Swanson, NIST
John Tressler, DoED, TAR
Becky Vasvary, NOAA, AC

TAR - denotes target agency representative
AC - denotes agency coordinator

SPECIAL THANKS

A special thanks to all those who took the time to complete a needs assessment form or to participate in a needs assessment interview. Special thanks also to the target agency representatives for their contributions throughout the design and conduct of the study. Thanks to the agency coordinators and others who identified respondents and interviewees, or who coordinated the distribution and collection of the surveys or arranged for interview meetings. Additional thanks to the study working group members for their initial and continued input.

NIST
FEDERAL AGENCY
INFORMATION TECHNOLOGY (IT)
SECURITY NEEDS STUDY

TABLE OF CONTENTS

LIST OF TABLES

LIST OF APPENDICES

SECTION I.
INTRODUCTION

A. Introduction

Changes in information technology (IT) have significant impact on how organizations do business. The federal government has long recognized the value of its information and its IT resources. Federal directives issued during the past two decades have addressed IT development, acquisition, use, and management. More recently, as change has accelerated and the use of IT has become even more fundamental, awareness of sensitive information, systems, and applications has increased. This awareness goes hand-in-hand with an improved understanding of the threats to and vulnerabilities of IT assets and the need to protect them. (Note that for the remainder of this study report, the term *"security"* refers to *"IT security."*)

Federal agencies and other organizations are faced with a variety of requirements concerning the protection of sensitive information and the resources used to store and process that sensitive information. These security requirements derive from a number of sources, including legal and regulatory responsibility; Privacy Act and other privacy concerns regarding employees, clients, and customers; fiduciary and custodial responsibility; national security; desire for public, client, and customer confidence; good management and business practice; fear of fraud and embezzlement; fear of litigation and increased regulation; and ethical concerns. The rapidly changing IT environment and a number of short-term and long-term trends raise new IT protection concerns and challenges.

What are these needs and requirements? How do we determine what help agencies and other organizations need to address these requirements? What resources are available to help and what are the means to focus resources appropriately? A number of recent efforts attempt to address these questions. The study is one such endeavor.

B. Purpose, Scope, and Intended Audience

The National Institute of Standards and Technology (NIST) is chartered with helping federal agencies meet their individual security requirements. It is of critical importance that NIST has an accurate understanding of what agencies need to

meet those requirements in order to more effectively structure its security program. To improve its ability to identify and assess agency needs, NIST conducted a study which involved interviews with federal agency staff and the use of an security needs assessment survey. Respondents identified their security needs from a list of candidate needs and indicated the importance and immediacy of each. Federal, private sector, and professional organizations took part in the study. Also, a study working group representing the federal and private sectors participated in the design of the study and the validation of study results.

The results of the study will help NIST more fully understand the security needs of federal agencies, affirm NIST planned research, support, and outreach activities, and provide a sound basis for future planning of NIST's security program. The study results also provide a base for an on-going assessment of federal agency security needs.

This study focused primarily on the needs of federal agencies to address their non-classified security requirements. The results of the study and NIST's response, however, may be applicable to a wider audience that includes interested parties in the private sector. (See NISTIR 4976, Assessing Federal and Commercial Information Security Needs, regarding similarity and differences between the federal and private sectors.)

The remarks of study participants were not limited to those areas definitely within NIST's scope and charter, but include concerns that fall within the purview of other central agencies. The study team thought it useful to pass these along. As can be seen in Section V, Conclusions, some of the identified needs are more appropriately addressed by other organizations.

A primary intended audience of this study is NIST security management. Among other potential audiences are those agency staff concerned with security management, policy, planning, implementation, and training who want to either consider their security needs or provide input to those who may represent a source of help.

C. Security "Needs" vs. "Requirements"

For the purpose of this report, a distinction is made between security "requirements" and security "needs." As used in this report, security "requirements" are levied on an agency or an organization from an external source, e.g., Office of Management and Budget (OMB) Circular A-130, Appendix III. Requirements

encompass WHAT security action is to be done, and perhaps WHY. "Needs" encompasses understanding the HOW, WHO, and HELP sought in meeting the requirements, e.g., guidance on how to do contingency planning. It is assumed agencies know their requirements, but look for help to meet these requirements.

D. Related Activities and Documents by NIST and Others

Recent activities by NIST and others provided background and additional understanding of agency security needs. These include:

- Computer security curriculum development efforts by the Federal information system Security Educators' Association (FISSEA) (See Appendix K.)

- Office of Management and Budget (OMB), NIST, and the National Security Agency (NSA) agency assistance visits made in accordance with OMB Bulletin 90-08 (and the results of the NIST and NSA Computer Security and Privacy Plans review effort done in accordance with OMB Bulletin 88-16) (See Appendix D.)

- NISTIR 4976, Assessing Federal and Commercial Information Security Needs, detailing similarities and differences between the federal and private sectors. This NIST study discusses the technical information protection methods used in computers or application systems in government and industry. The study involved meetings and discussions with key persons in 17 federal agencies, 10 commercial organizations, and one state government, between March and June 1991. Approximately 120 people were interviewed. The study provides input to NIST's Minimum Security Requirements and Federal Criteria efforts. (See Appendix I.)

- The NIST Framework Handbook effort (See Appendix I.)

- The NIST Integrated OSI, ISDN, and Security Program (See Appendix I.)

- The President's Council on Integrity and Efficiency produced a Model Framework for computer security addressing a list of 55 controls.

- Computers at Risk: Safe Computing in the Information Age, produced

by the National Research Council's System Security Study Committee

(Also see Appendix F.)

E. Overview of the Document

Section I provides an introduction and background into the NIST agency security needs study. Section II describes the approach and methodology of the study. Section III presents an analysis of the survey data. Section IV presents the results of the interviews and other study findings. Section V contains conclusions and recommendations. A series of Appendices provide supplementary detailed information and a set of references that may be of value to the reader.

SECTION II.
APPROACH AND METHODOLOGY

A. The Study Working Group and the Initial Planning Meeting

In order to get a broad perspective and support for the study, NIST hosted a meeting of invited participants in February 1992 to review and comment on the study approach and methodology and to provide ideas and suggestions for improving the study plan. This **study working group**, consisting of approximately 30 federal and private sector representatives, provided direction to the study. The group met again in September 1992 to review the study results. This study report reflects the study working group input. (See Appendix E for a listing of attendees at the February 1992 planning meeting and the September review meeting.)

B. Overall Approach and Methodology

Based on the results of the February 1992 planning meeting, the study team developed an approach and methodology, which included:

- reviewing existing documented requirements and needs
- conducting a survey of federal agency security needs
- interviewing agency staff regarding their security needs

C. Use of Target Agencies, Target Agency Representatives (TARs), Surveys, and Interviews

The study focused on five **target agencies**, selected because they represent a variety of federal security environments. These agencies are the Department of Commerce, Department of Education, Department of Justice, National Aeronautics and Space Administration, and Social Security Administration. (NOTE: Originally there were four target agencies, with Department of Education joining after the start of the process.) It was agreed the study would involve interviews with agency staff, identified by representatives of the target agencies, and the use of an security needs assessment survey. After informal consultation, a formal request for participation was made by NIST to the target agencies. (See Section

III.B regarding a limited distribution of surveys beyond the target agencies. Also see Section III.B for a summary of the number of survey responses and interview meetings held with each of the target agencies.)

Each **target agency representative (TAR)**, the prime contact from each target agency, had significant duties and responsibilities which encompass security. Based on a number of meetings with these representatives, and input from the study working group, an security needs assessment survey form was developed by the study team. The survey asked respondents to indicate the importance and immediacy of each of three dozen candidate needs. There was also opportunity provided to elaborate on the candidate needs, specify other needs, or offer comments. (The survey was based, in part, on the responses to a questionnaire that was completed by members of FIRMPOC in early FY 1992. That questionnaire, which used an open-ended format, requested information on what NIST could do to support agency security efforts. All of the target agencies had participated in the FIRMPOC survey. See Appendix A for a list of needs expressed in the FIRMPOC questionnaire responses.)

In consultation with the **study team**, which consisted of the TARs and the NIST project coordinator, each TAR identified those who should receive surveys and who should be interviewed. The question of how many were left up to the TARs. (See Section III.B for information regarding the types of study participants and also see Appendix L for a list of job titles or responsibilities of those interviewed.) The TARs were instructed that those selected should reflect diverse security environments. (Note: The study team was occasionally augmented by NIST staff for the interviews.)

It was also emphasized that it was not the "agency" that was being surveyed or interviewed, but rather a set of individuals, who collectively with those from the other target agencies, would communicate security needs from a variety of federal perspectives, applications, and security and data processing environments. The agency was not being "graded," reviewed, or audited in any way. The study team wanted to get input from security, information resources management (IRM), IT operations, and functional or applications systems. The study team also wanted to get management, administrative, and technical perspectives. It was explained that no one meeting or group would necessarily address all of these perspectives.

It was emphasized that all agency protocols, idiosyncracies, and ways of doing business would be respected. Respondents and interviewees were encouraged to view the interviews and needs assessment survey as opportunity rather than a

"have to" chore.

The TARs discussed a concern that if surveys were returned through a management chain, there was a possibility they would get "sc ed." Most of the TARs opted to have the surveys sent directly to NIST, with the da being available to the TARs if they desired, subject to confidentiality considerations discussed below.

Given all these considerations, the TARs were asked to develop a plan for completing the surveys for their agency, including milestones. Although not required to do so, each of the TARs decided to use their existing security organization, structure, or distribution channels for the distribution of the surveys.

Surveys were distributed in May and June 1992. Concurrently, interviews, except for Department of Education, were conducted and completed by late June. Explored in the interviews were the individuals' primary security issues, concerns, and problems - in terms of impact on the organization's ability to conduct its business and perform its mission. Nearly all interviews were attended by the NIST study team and the TAR from the organization being interviewed. Interviews generally lasted from one to two hours.

(Note: An individual experienced with survey instruments was consulted in developing the survey. Also, there was consensus among TARs regarding the process for survey distribution and identifying interviewees. The criteria of reasonableness was applied, but beyond that, no attempt was made to achieve statistical validity in the study. It was felt an objective of the approach and methodology - to obtain input that represented a variety of federal security and IT environments and staff perspectives - was achieved.)

A draft study report was prepared and another meeting of the study working group was convened in September 1992 to discuss the study and its conclusions. This report reflects the input from the study working group.

D. Anonymity of Survey Responses and Interviews

Study participants were informed their involvement was strictly voluntary, the study was not part of an audit or Computer Security Act (PL 100-235) security and privacy plans review effort, the study team was looking for candid input, and requests for anonymity would be honored. To encourage candid replies, respondents were given the opportunity of requesting anonymity. Forty percent

either explicitly requested anonymity or did not provide identifying information.

SECTION III.
ANALYSIS OF SURVEY DATA

A. Introduction

The data collected from the federal agency security needs assessment survey is presented in this section in narrative and tabular form. This information is supplemented with more detailed material in the referenced appendices. The data is further examined in Section IV, where it is discussed in conjunction with the results of the study interviews and additional needs and comments made by survey respondents. (Note: In the tables in Section III, percent data may not add up to 100 percent, because of rounding. However, 100 is used as the percentage for the total number of responses.)

B. Profile of Survey Responses and Respondents

A total of 224 survey responses were received. The vast majority of these (88 percent) came from the target agencies. The table below shows the distribution of survey responses from the target agencies.

TABLE III-1
TARGET AGENCY SURVEY PARTICIPATION IN THE AGENCY SECURITY NEEDS STUDY

Source of Response	Number of Survey Responses	Percent of Total
Department of Commerce	73	33
Department of Education	37	15
Department of Justice	42	19
National Aeronautics and Space Administration	4	2
Social Security Administration	41	19
Number of Target Agency Responses	197	88
Number of Non-target Agency Responses	27	12
Total Number of Responses	224	100

Other federal, private sector, and professional organizations were invited to respond to the needs assessment by completing the survey form. Surveys were distributed to the study working group, members of the Federal Computer Security Program Managers' Forum, and a number of others who made requests. There was some overlap among the groups. Unfortunately, few besides the target agencies chose to respond to the survey. One other agency provided approximately 5 percent of the responses. Only 1 response was clearly identifiable as non-government, with federal agencies representing fully 99 percent of the responses. It should be noted two of the surveys indicated they represented agency or "corporate" positions. (See Appendix X for a complete count of survey responses by agency or organization affiliation.)

Respondents indicated they received their surveys from two primary sources - either from their agency sponsor (63 percent) or directly from NIST (14 percent).

TABLE III-2
DISTRIBUTION OF RESPONSES BY HOW RESPONDENT RECEIVED THE NEEDS ASSESSMENT SURVEY

How Survey Was Received	Number	Percent
From agency or organization sponsor	140	63
Via NIST Computer Security BBS	1	0
Directly from NIST	31	14
Other or undetermined	49	22
TOTALS	224	100

The following is the distribution of responses by government grade designation. The results indicate the survey received attention from high level management. A significant portion of the total responses (50 percent) were submitted by employees at the GS/GM-14 level or above. A government grade could be determined for 80 percent of those who submitted surveys.

TABLE III-3
DISTRIBUTION OF RESPONSES BY GOVERNMENT GRADE DESIGNATION

Government Grade	Number	Percent
GS/GM-12 or lower	30	13
GS/GM-13	40	18
GS/GM-14	58	26
GS/GM-15	46	21
SES	6	3
Other or undetermined	44	20
TOTALS	224	100

The following table provides a distribution of survey responses by title, occupation, position, or area of concern. It appears a variety of relevant perspectives were represented among the survey responses. (See Appendix L for a full list of represented titles, occupations, positions, or areas of interest.)

TABLE III-4
DISTRIBUTION OF RESPONSES BY TITLE, OCCUPATION, POSITION, OR AREA OF CONCERN

Title, Occupation, Position, or Area of Concern	Number	Percent
Computer Security Officer	62	28
Computer/DP Management	29	13
Director	20	9
Functional/Line Management	20	9
IRM	14	6
System Analyst	13	6
Other	66	30
TOTALS	224	100

The following table shows the distribution of survey responses by the identified security-related experience. It is not readily apparent why there were so few total responses to this environment profile question (only 52 percent) or why there are no responses to one to three years experience. It is interesting that approximately one third of all respondents and two fifths of those who answered this question indicated less than one year experience. This may reflect the way security assignments are made. It could indicate security is often a secondary duty and staff are rotated through the assignment for brief periods of time.

TABLE III-5
DISTRIBUTION OF RESPONSES BY SECURITY-RELATED EXPERIENCE

Years of Experience	Number	Percent
None	1	0
Less than 1 year	73	33
1 to 3 years	0	0
3 to 5 years	41	19
5 to 10 years	2	1
Over 10 years	2	1
No response, other, or undetermined	105	47
TOTALS	224	100

The following table shows a profile of the target agency participation in the study interviews. (Note: Department of Education became a target agency late in the process and time and scheduling constraints precluded conducting interviews with their staff.)

TABLE III-6
TARGET AGENCY INTERVIEW PARTICIPATION

Target Agency	Number of Interview Meetings	Number Interviewed
Department of Commerce	4	39
Department of Education	0	0
Department of Justice	4	16
National Aeronautics and Space Administration	1	9
Social Security Administration	3	23
Target Agency Totals	12	87

C. Respondent Ratings of Survey Candidate Needs

In order to help respondents structure their thinking about their needs, the 36 candidate needs from the survey were organized and presented in four groups, with each candidate need having a need number associated with its group. The candidate needs appearing in each group are given in Table III-7. The first group contains *needs related to policy, management, and planning.* The second group contains *needs related to basic security functions and activities.* The third group contains *needs related to technical approaches, methodologies, and products.* The fourth group contains *needs related to the access to and sharing of security information.* The first group was further subdivided in to *federal policy* and *agency security, management and planning.* The third group was further subdivided in to *area of concern* and *specific security environments.* (See Appendix B for a copy of the survey and a fuller description of the candidate needs.)

Respondents reported both importance and immediacy ratings for each candidate need. However, based on the interviews, it appears respondents gave

more attention to responses related to importance than to those related to immediacy. Not surprisingly, though, there was a strong relationship between importance and immediacy in survey responses. That is, higher levels of importance of candidate needs had associated ratings of greater immediacy, meaning respondents reported needing them sooner on the average. The rest of the analysis in this section and in Section IV is based primarily on importance responses. (See Appendix N and Appendix O for the overall distribution of and relationship between importance and immediacy survey responses.)

Table III-7 also shows the percentage distribution of importance responses. It is presented in candidate need number order and grouped as described above.

(Note: In Tables III-7 and III-8 and in the appendices *"No Resp."* or *"No Response"* means no response was given in that percent of survey responses. Also note Tables III-7 and III-8 are continued on second and third pages.)

KEY TO TYPE OF CANDIDATE SECURITY NEED: A=assistance; G=guidance; P=policy; PR=products; S=standards; TA=technical approaches; TI=technical information

TABLE III-7
PERCENTAGE DISTRIBUTION OF IMPORTANCE RATINGS OF CANDIDATE NEEDS

Need No.	Candidate Need	Importance					
		No Resp.	None or Not Appl.	Low	Mod-er-ate	High	Very High
Needs Related to Policy, Management, and Planning							
Federal Policy							
A01	P/G-integrating ITS policies and directives	5	4	20	32	28	11
A02	P-owner of sensitive systems	3	7	21	31	29	9
A03	P/G/TR-executive/mgt SA&T	4	6	15	33	31	12
A04	P-putting ethics in OPM regs	7	12	26	34	18	3
A05	P-ITS in system development life cycle	3	3	16	33	29	15

TABLE III-7
PERCENTAGE DISTRIBUTION OF IMPORTANCE RATINGS OF CANDIDATE NEEDS

Need No.	Candidate Need	Importance					
		No Resp.	None or Not Appl.	Low	Mod-er-ate	High	Very High
A06	P-collection, dissemination, sharing	3	4	21	33	27	12
A07	P-emergency response capability	4	9	17	28	34	8
Agency Security Management and Planning							
A08	G-agency ITS policy	4	7	21	38	23	6
A09	G/S-defining sensitive systems	4	5	17	30	31	12
A10	G-developing security plans	4	5	17	32	33	8
A11	G-management-level ITS planning	4	9	16	34	28	9
Needs Related to Basic Security Functions and Activities							
B01	G/PR/A-risk analysis	2	7	20	29	28	14
B02	G/A-contingency and disaster recovery plans	4	7	13	30	34	13
B03	G/TA/A-impact of security violations	3	4	25	32	29	8
B04	G/A-disaster recovery testing	5	10	20	34	22	9
B05	G/A-emergency response capability	6	8	23	32	25	5
B06	G/A-independent security verification reviews	5	8	28	31	22	5
B07	G/A-certification and accreditation	6	11	26	29	20	9

TABLE III-7
PERCENTAGE DISTRIBUTION OF IMPORTANCE RATINGS OF CANDIDATE NEEDS

Need No.	Candidate Need	Importance					
		No Resp.	None or Not Appl.	Low	Mod-er-ate	High	Very High
B08	G/A-comprehensive personnel security pgm.	4	14	28	29	20	6
B09	G/PR/A/materials-Security Awareness and Trg.	4	5	18	38	26	10
Needs Related to Technical Approaches, Methodologies, and Products							
Area of Concern							
C01	TA/PR-access control and authentication	5	10	23	31	22	9
C02	TA/G-public access by client populations	6	11	29	25	25	5
C03	G/PR-individual user accountability	6	8	21	33	24	8
C04	G/S-minimum controls for sensitivity levels	3	8	23	29	25	11
C05	PR/S-satisfying (inter)national criteria	9	21	29	27	10	4
C06	G/PR/TA-troubleshooting ITS problems	4	11	22	29	22	11
C07	G/PR-EDI, PKE, DS, and elec. authentication	5	8	21	31	22	13
C08	TA/PR-ITS in s/w development and s/w engrg	5	9	21	27	29	10
C09	TI-computer security tools (evaluations)	5	7	17	43	22	7

TABLE III-7
PERCENTAGE DISTRIBUTION OF IMPORTANCE RATINGS OF CANDIDATE NEEDS

Need No.	Candidate Need	Importance					
		No Resp.	None or Not Appl.	Low	Mod-er-ate	High	Very High
	Specific Security Environments						
C10	S/G/TA/PR-LANs	4	6	8	16	42	25
C11	G/PR/TI-linking PCs/LANs/MFs in 1 ITS arch	3	6	8	21	37	24
C12	G-integrating open system products	6	9	13	32	27	13
C13	G/TA-secure dial- in and laptops	4	9	15	22	36	14
C14	G-database security	2	6	14	25	34	18
	Needs Related to Access to and the Sharing of Security Information						
D01	Clearinghouse of ITS information	5	8	15	36	25	11
D02	Better flow of info from NIST to constituency	8	10	18	30	23	10

In order to rank and further analyze the candidate needs, letter designations used by respondents to report importance and immediacy of each candidate need were converted to numbers. Based on these numbers, a "weighted" average importance value and a "weighted" average immediacy value was calculated for each of the 36 candidate needs. (See Appendix P for the specifics of this calculation.)

The following table presents the percentage distribution of importance ratings for each candidate need. It is in descending order by the calculated average importance value for all responses for each need (i.e., a ranking of number 1 indicates the highest importance rating and a ranking of number 36 indicate the lowest importance rating. Ratings of *no importance, not applicable,* or *low*

importance are grouped together, as are those of *high importance* and *very high importance. The groupings were done to more clearly show patterns in importance ratings. (See Appendix Y for an ungrouped version of this table.)*

(Note that in Table III-8 the top, middle, and bottom thirds of the ranked needs are separated by a thick line.)

KEY TO TYPE OF CANDIDATE SECURITY NEED: A=assistance; G=guidance; P=policy; PR=products; S=standards; TA=technical approaches; TI=technical information

TABLE III-8
PERCENTAGE DISTRIBUTION OF GROUPED IMPORTANCE RATINGS OF CANDIDATE NEEDS IN DESCENDING ORDER BY AVERAGE IMPORTANCE

Rank	Need No.	Candidate Need	Importance			
			No Resp.	None, N/A, or Low	Mod-er-ate	High or Very High
1	C10	S/G/TA/PR-LANs	4	14	16	67
2	C11	G/PR/TI-linking PCs/LANs/MFs in 1 ITS arch	3	14	21	61
3	C14	G-database security	2	20	25	52
4	A05	P-ITS in system development life cycle	3	19	33	44
5	B02	G/A-contingency and disaster recovery plans	4	20	30	47
6	C13	G/TA-secure dial- in and laptops	4	24	22	50
7	A03	P/G/TR-executive/mgt SA&T	4	21	33	43
8	A09	G/S-defining sensitive systems	4	22	30	43
9	A10	G-developing security plans	4	22	32	41
10	B01	G/PR/A-risk analysis	2	27	29	42
11	C12	G-integrating open system products	6	24	32	40

TABLE III-8
PERCENTAGE DISTRIBUTION OF GROUPED IMPORTANCE RATINGS OF CANDIDATE NEEDS IN DESCENDING ORDER BY AVERAGE IMPORTANCE

Rank	Need No.	Candidate Need	Importance			
			No Resp.	None, N/A, or Low	Mod-er-ate	High or Very High
12	A06	P-collection, dissemination, sharing	3	25	33	39
13	A01	P/G-integrating ITS policies and directives	5	24	32	39
14	B09	G/PR/A/materials-Security Awareness and Trg.	4	23	38	36
15	D01	Clearinghouse of ITS information	5	23	36	36
16	A07	P-emergency response capability	4	26	28	42
17	C07	G/PR-EDI, PKE, DS, and elec. authentication	5	29	31	35
18	A02	P-owner of sensitive systems	3	28	31	38
19	A11	G-management-level ITS planning	4	25	34	37
20	B03	G/TA/A-impact of security violations	3	29	31	37
21	C08	TA/PR-ITS in s/w development and s/w engrg	5	30	27	39
22	C04	G/S-minimum controls for sensitivity levels	3	31	29	36
23	C09	TI-computer security tools (evaluations)	5	34	43	29

TABLE III-8
PERCENTAGE DISTRIBUTION OF GROUPED IMPORTANCE RATINGS OF CANDIDATE NEEDS IN DESCENDING ORDER BY AVERAGE IMPORTANCE

Rank	Need No.	Candidate Need	Importance			
			No Resp.	None, N/A, or Low	Mod-er-ate	High or Very High
24	D02	Better flow of info from NIST to constituency	8	28	30	33
25	C03	G/PR-individual user accountability	6	29	33	32
26	B04	G/A-disaster recovery testing	5	30	34	31
27	A08	G-agency ITS policy	4	28	38	29
28	C06	G/PR/TA-troubleshooting ITS problems	4	33	29	33
29	C01	TA/PR-access control and authentication	5	33	31	31
30	B05	G/A-emergency response capability	6	31	32	30
31	B07	G/A-certification and accreditation	6	37	29	29
32	B06	G/A-independent security verification reviews	8	36	31	27
33	C02	TA/G-public access by client populations	6	40	25	30
34	B08	G/A-comprehensive personnel security pgm.	4	42	29	26
35	A04	P-putting ethics in OPM regs	7	38	34	21
36	C05	PR/S-satisfying (inter)national criteria	9	50	27	14

D. Consistency of the Rankings

While the calculations of average importance do produce a ranking of candidate needs, in some cases the difference from one ranked need to the one above it or the one below it, is very small. However, it does appear there is an overall pattern which shows a markedly stronger preference for those candidates needs whose average importance ranked the highest average over those candidate needs ranked near the bottom. For the most part this was borne out in the interviews and in discussions with the TARs and the study working group members.

(See Appendix S for the actual calculated average importance and immediacy values. Also see Appendix T for the values from Appendix S "normalized" to the overall average importance and average immediacy values. Also see Appendix U for a presentation of the variations of average importance values in terms of calculated averages, normalized averages, number of standard deviations each average importance value is from the overall mean or average importance value for all responses, and the percentage of total responses that rated each candidate need *highly* or *very highly important*.)

In order to see if responses differed with government grade, the importance values of candidate needs for all respondents (224) were compared with those who indicated their government grade was GS/GM-13/14 (98) or GS/GM-15, SES (52). The average importance rating for each candidate need was calculated. The candidate needs for each group were then ranked from 1 to 36 or from high to low importance (with 1 being highest average importance and 36 being the lowest average importance). A comparison was then made to see if noticeable differences exited in the way the three groups (i.e., All, 13/14, 15/SES) rank each of the 36 candidate needs . Appendix R shows differences among the ratings for each group for each candidate need. In Table III-9, a subset of Appendix Q, the candidate needs with differences of 10 or more between the 13/14 and the 15/SES rankings are shown.

KEY TO TYPE OF CANDIDATE SECURITY NEED: A=assistance; G=guidance; P=policy; PR=products; S=standards; TA=technical approaches; TI=technical information

TABLE III-9
RANKING OF IMPORTANCE OF CANDIDATE NEEDS AMONG ALL RESPONDENTS AND SELECTED GOVERNMENT GRADES

Need No.	Candidate Need	Over-all Rank	Rank for 13/14	Rank for 15/SES
A09	G/S-defining sensitive systems	8	8	19
A10	G-developing security plans	9	3	22
C12	G-integrating open system products	11	26	6
D01	Clearinghouse of ITS information	15	15	25
A11	G-management-level ITS planning	19	16	30
A08	G-agency ITS policy	28	17	35
B07	G/A-certification and accreditation	31	34	23

The three groups viewed many needs similarly in terms of importance. However, there were some notable differences. For example, Table III-9 shows the 15/SES group ranked candidate needs:

- C12 (guidance on integrating open systems products) and
- B07 (guidance and assistance related to certification and accreditation)

substantially more important than the 13/14 group. (These two candidate needs are shaded in the table.)

The table also shows the 13/14 group ranked candidate needs:

- A08 (guidance on developing agency security policy),
- A09 (guidance and standards on defining sensitive systems),
- A10 (guidance on developing security plans),
- A11 (guidance on management-level security planning), and
- D01 (clearinghouse of security information)

substantially higher (i.e., more important) than their 15/SES counterparts. It is interesting to note A08-A11 are the four candidate needs directly related to agency security management and planning.

SECTION IV.
FINDINGS, OBSERVATIONS, AND DISCUSSION

A. Some General Comments Regarding the Survey, the Interviews, and the Study

Some people are looking for the "silver bullet" for their security concerns, and, of course, there is none. The good news is, however, there were very few of these people among those interviewed and much of the help requested in the interviews and survey responses already exists or is being developed by NIST and others. Also, many agencies are making a significant effort to identify and solve their security problems.

Many security needs were expressed in the course of the study. Some were simple. Some were complicated. Some were tangential. Many were fundamental. Most were interrelated. The study team noted only 24 percent of the surveys expressed one or more additional needs and only 13 percent provided additional comments.

A number of those interviewed expressed appreciation at the opportunity to focus on security, and also to discuss their problems and frustrations. A number of people said they saw the survey as a tool they could use to better understand the security needs of their constituency.

B. Overall Survey Results

B.1 Summary of Survey Results

The following is a summary of the ratings of subgroups of candidate needs based on their calculated average importance. (See Table III-7 and Appendix V.) It should be noted, for the most part, the interviews and additional comments from respondents supported the survey results. However, there were instances where persons interviewed voiced somewhat differing priorities.

Overall, needs related to technical approaches, methodologies, and products were rated higher in average importance then other subgroups of candidate needs. Needs in this group, in turn, consisted of a subgroup addressing specific security environments and a subgroup addressing particular areas of concern and

subgroups addressing. The security environments subgroup included needs related to *LANs, linking systems in one security architecture, integrating open system products, secure dial-in and laptops*, and *database security*. This subgroup provided the strongest showing as a subgroup.

The particular environments subgroup included needs related to *access control and authentication, public access by client populations, individual user accountability, minimum controls for sensitivity levels, satisfying (inter)national criteria, troubleshooting security problems, security in software development and software engineering*, and *computer security tools evaluations*. This subgroup had the lowest average as a subgroup. Only candidate need C07, *guidance and products related to electronic data interchange, private key encryption, digital signatures and electronic authentication*, was slightly above the overall average.

The group of candidate needs related to policy, management, and planning consisted of a subgroup of needs addressing federal policy and a subgroup of needs addressing agency security management and planning. The needs in the group were rated at or above the calculated average importance for all candidate needs. The one exception was candidate need A04, *policy on putting ethics in OPM regulations*, which ranked substantially below the average.

Overall, needs related to basic security functions and activities were rated lower than average. Only needs B01, *guidance, products, and assistance with risk analysis*, B02, *guidance and assistance with contingency and disaster recovery plans*, and B09, *guidance, products, assistance, and materials for security awareness and training*, did better than the average.

Together, the group of needs related to accessing and sharing security information was just at the overall average. One candidate need in the group, D01, *clearinghouse of security information*, was a little above the average. The other candidate need in the group, D02, *better flow in information from NIST to its constituency*, was a little below average.

B.2 A Low Importance Rating in the Survey Does Not Mean that the Subject Is Unimportant

It is important to note a relatively low importance rating does not mean the subject of the need or the underlying requirement is not important. It may simply be a statement about the importance of help to a respondent in addressing a particular requirement. For example, there is agreement on the importance of security awareness and training. However, if this area is "under control," then a

respondent could rate the importance of external help in this area as low. It should also be noted a relatively low importance rating may be caused by less than full appreciation and knowledge of the importance or long-term value of a particular subject.

C. Discussion of Findings and Observations

Below is a summary of the findings and observations made during the agency security needs study. Appendix M contains additional material from the interviews and comments made by survey respondents. Each section below represents a collection of related thoughts. As may be expected, remarks made in the interviews and additional comments offered by survey respondents do not fall into neat, distinct categories. Overlaps and interrelationships among issues exist. It is the opinion of the study team that some of the remarks made by study participants may be based on an incomplete or inaccurate understanding on the part of the respondents or interviewees, or the result of misinterpretations or miscommunications among study participants and the study team. However, understanding where study participants lack a full appreciation of what is required and what resources are available may provide insight into how best to serve federal agencies. Also note that opinions reported here are not necessarily shared by NIST or the study team members. Departures from a full understanding of what is required and what resources are available on the part of some study participant may provide insight into how best to serve federal agencies. Wherever *"disconnects"* exist, they need to be recognized, understood, and addressed.

The sections here and in Appendix M are loosely organized to correspond to the major groupings of candidate needs as presented in the needs assessment survey. (See Table III-7.) However, there is not a one-to-one mapping of the discussion sections and the candidate needs as presented in the survey. This is due to the fact some subjects were raised in the interviews that did not readily lend themselves to a particular candidate need and suggested a different grouping.

C.1 General

C.1.a Concern was Expressed about Dealing with New and Changing Technical and Processing Environments

One of the major concerns of interviewees was facing the new and changing

technical and processing environments. In some cases, the changes were evolutionary. In other cases, changes were occurring more dramatically. Many expressed concern about how they would carry out their security responsibilities under these changing conditions. They indicated they are looking for help in anticipating what the new technology will bring so they can better understand the new threats and vulnerabilities and be ready with commensurate protections. Those interviewed said they wanted to be able to look toward the future - and transition to what is coming. How does an agency change directions? They also wanted technical details about future security products.

Among the new and changing environments mentioned were more work being performed at home (telecommuting), increased citizen access to government data and services, major system modernization projects, more work being over telephone lines, increasing use of PCs as front-ends in major processing systems, more automation of functions, more electronic distribution of functions, more extensive use of networks, use of very large and distributed data bases, greater use of electronic documents, and a continuing migration to open systems environments.

C.1.b A More Detailed Understanding of Security Requirements is Desired

Among those interviewed, there appears to be a reasonable level of awareness and comfort with the general notion of security requirements and the federal directives from which they flow. However, considerable concern, even frustration, was expressed about what is expected of an agency under current policy and guidance and with the specific meaning of the requirements and how these requirements were to be translated into action. Interviewees wanted to know specifically what was expected and how that would be measured. The need for a common interpretation of requirements was often repeated by participants.

C.1.c It is not Clear Where to Most Effectively Focus Security Policy, Guidance, Training, and Assistance

Given the great diversity of security environments among and within agencies, it was unclear how to most effectively target security policy, guidance, training, and assistance. At what level and in what form can help be best delivered? Ideally, interviewees look for policy and guidance that is neither too general nor too specific. If requirements and help are too general, they run the risk of being bland and meaningless. If they are too specific, they may ignore the practical realities of individual environments and lack sufficient flexibility. Interviewees

acknowledge achieving the correct mix is difficult to accomplish.

A number of interviewees felt system owners, whom the interviewees considered the most knowledgeable about the system, should make the security decisions. They felt this should be done at the lowest level appropriate to the situation and this is where attention and help should be focused. One way to accomplish this suggestion is by providing examples based on a "common" configuration, situation, or environment - and then let the user make the necessary situation-specific or environment-specific adjustments.

C.1.d "Filtering" is Wanted by Users Less Sophisticated about Security Issues and Concerns

A number of interviewees noted help to users needs to take into account differences in experience and sophistication among users. In many cases, we are dealing with users less sophisticated about security issues and technology. At each of the levels within the agency at which security is implemented, there needs to be appropriate "filtering" or simplifying. It did not appear to be of particular significance who did the "filtering." However, there was also some discussion as to the optimum placement of this *"filtering of material"* support. A number of interviewees felt, because of limited resources, this could be best implemented at the agency level, rather than at a subunit level.

Users and data owners wanted to be informed of problems and provided with simple, easy to use tools. Those responsible with helping others with security, wanted to know how to get the right information to the right people.

The area of security for PCs and multi-user systems was identified as one in which help is needed. Interviewees said having a agency-wide or governmentwide place to call to get security information and assistance would be helpful. The model of a PC help desk or user assistance office was noted as one that was successful and had user support. One suggestion was to have a place where a system administrator could call up for product-specific information for security products and tools. Such a centralized resource person is needed to help configure new multi-user workstations with all the necessary patches. This person would get the system administrator *"up to speed"* and help maintain and distribute patches for all users. Having access to a *"resource desk"* or *"help desk"* covering categories of information and using a 1-800 number was among the possibilities offered. Some even raised the possibility of the use of a 1-900 number as a possible way of paying part of the cost of such a service.

C.2 Issues Concerning Security Policy, Management, and Planning

C.2.a Many Feel Hampered by Limited Resources and Budgets and Frustrated in Justifying Security Resources

A number of those interviewed said they did not have enough resources (dollars, people, equipment) to do their jobs effectively. They said security was competing with other management and programmatic needs and was not doing well in the competition. They felt requirements were being placed on them, without the commensurate resource support. This issue was frequently introduced with, "*You probably can't do anything about this, but....*" Interviewees saw this as a continuing problem.

It was felt the lack of resources for security had a number of causes, including competition for the same limited resources. Another was an incomplete understanding on the part of management of the role of security. It seemed especially difficult to justify staff. In general, those who were interviewed expressed confidence their people were capable of performing the necessary security functions, but also voiced concern that there were not enough people to do all of the work. A number of interviewees said they would like to see NIST help them justify the need for an security program and supporting staff. Some thought this could be done indirectly by helping to increase the level of security awareness on the part of executive and functional managers. (See discussion on security awareness and training of executives in Sections C.4.b) Some interviewees wanted a separate security budget in order to get appropriate attention and response from management.

In a survey of 154 security staff conducted by Government Computer News and reported on in their October 12, 1992 issue, lack of resources was the most common explanation offered by respondents for inadequate security programs.

In regard to dealing with security budgets and resources, many of those interviewed wanted to know what others are doing in similar situations.

C.2.b Interviewees are Concerned about Addressing Security in an Environment of Competing (Production and Other) Demands

One of the issues frequently raised in the interviews was of the conflicting demands faced by those responsible for implementing security. Security is

required for an organization to perform its mission. Management and users often fail to recognize this role of security. The *"political"* environments of some organizations result in security being paid *"lip service"* and tolerated as long as it does not interfere with production schedules.

Many interviewed reported users and clients complain security slows system response time. This is a particular concern in high volume, mission critical, or potentially life-threatening situations. The interviewees were looking for products and methods to achieve desired levels of both security and performance. Some saw the need for guidelines that identify a comprehensive security policy without adversely affecting system operations or production capability.

A number of those interviewed felt their immediate management thinks security is critical, but they were concerned their upper management doesn't see any value-added results or savings. Given the lack of an apparent payoff, the managers don't want to burden their staffs. Some thought including security in Management by Objective (MBO) performance elements, other performance plans, and position descriptions would be a step in the right direction. (See discussion on security awareness and training of executives in Sections C.4.b.)

C.2.c *Interviewees Want Federal and Agency Security Requirements to be Reasonable and Relevant. They Want Realistic, Practical, Integrated Federal Security Policy, Directives, and Guidance*

One purpose of federal and agency policy and directives is to explicitly define "acceptable" and "unacceptable." Another is to provide a context in which certain behaviors are "expected." Policy should provide an understanding which creates the incentive for the desired behaviors. Interviewees said "good" policy and guidance should answer the question of "Why security?" by clearly communicating to the reader: *It makes sense. It's consistent with good management and business practices. IT'S THE LAW!*

Many thought policy should sustain and encourage good management practices. Survey responses showed most of the candidate needs that directly addressed federal policy ranked in the top third or middle third of the candidate needs.

Many interviewees expressed a willingness to respond to security requirements. However, they did expect these requirements should be reasonable and practical, contribute to accomplishing their mission, reflect an understanding and

appreciation of their specific situation and environment, and consistently integrate with IT management requirements. Some saw a need for general, consistent policy and guidance across networks, PCs, hosts, databases, and specialized services.

The need was loudly expressed for policy requirements that recognized the realities of the environments. Such policy should recognize the notion of "scalable" requirements - the notion that "one size fits all" is not always applicable in this arena. Guidance supporting policy would take into account variations in dealing with very small versus very large, complex systems. For example, some saw a need for a "scaling" of requirements for the security plans and other activities depending on the size and type of system and on the sensitivity of information or the sensitivity of the system. In general, the interviewees conveyed an appreciation of the actual or potential sensitivity of their systems.

Most looked to OMB to take the leadership role with regard to policy. Many also felt policy should be accompanied by guidance, tools, and other support agencies need to implement the policy. Many of those interviewed looked to NIST to play a leading role with respect to guidance in this area. Many of those interviewed looked to OMB, NIST, the agencies, and other members of the security community to work collaboratively to address federal security.

C.2.d Security Needs to be Integrated into Overall Management and Planning

Another of the really loud messages heard by the study team was that security is not an "island" unto itself, but rather an integral part of what an organization does and how it manages its resources, especially its IT resources. It was important to those interviewed that management take security seriously and view it in a larger context. They felt that executives and managers must be educated and their awareness raised about security to motivate them to *"do the right thing."* These executives and managers must also be aware of the role of policy, guidance, and tools to make the integration happen.

Many of those interviewed wanted to see security plans integrated into overall agency mission plans. They wanted to see all agency review requirements integrated, including those concerning IRM, internal controls, material weaknesses, and the Federal Managers Financial Integrity Act (FMFIA). Such integration would help security to more effectively compete with other agency objectives.

Without a full appreciation of security issues by management, there is a distinct

danger risk analyses and security plans will *"just sit on the shelf,"* and decisions will be made without the support and *"teeth"* only senior-level management can provide. Many of those interviewed indicated security needs to be a management priority. If it is looked upon as just an administrative and bureaucratic exercise, there is no value added.

C.2.e There were Varying Perspectives Regarding Additional External Security Requirements

The study team observed varying attitudes regarding whether security should be "required" (i.e., mandated) or, rather, whether it should be the subject of guidance.

The security people interviewed understood the value of protecting sensitive information and resources, and doing so was their direct responsibility. Some of these people wanted to be able to point to some documented authority when they are told by others, *"Show me where it says I have to do it. Otherwise, I have more pressing things to do."* They felt although there are existing laws and directives (e.g., the Computer Security Act and OMB Circular A-130), these did not fully serve the security people in these circumstances.

Some of these people felt that in their own environments security was well ingrained in the culture. They therefore were less likely to view external requirements to implement security as a burden. The requirements were more likely to be viewed in a larger IT context. It also appeared that such a view permitted a person requesting additional resources to do so more confidently.

Other interviewees, however, felt very strongly that additional requirements were not needed and current requirements were adequate. These people felt what would be helpful was meaningful guidance that would make it easier to do what they already know they needed to do. They felt additional security requirements would be burdensome and would make their jobs harder, not easier.

C.2.f Users are Concerned and Confused about Defining, Identifying, and Protecting Sensitive Information and Systems

This candidate need directly related to sensitive information and systems (need A09) was eighth in terms of rated importance and interviewees were very vocal about this subject. Some laws and directives such as the Computer Security Act and OMB Circular A-130 provide definitions of "sensitive," "sensitive information,"

"sensitive application," and "sensitive system." These laws and directives offer latitude to the agency in applying the definitions. As in other areas, the principles are understood at a high level. However, there is much confusion, uncertainty, and frustration as to how they should be applied in specific situations, or when they should be applied, how one knows if it has been done correctly, and who certifies as to the correctness. Many of the interviewees expressed a need for clearer definitions that are easier to apply in their environments. Some felt examples of how these terms are to be applied in real-world situations would be helpful.

Some of those interviewed felt they were constantly in the position of being second-guessed. They were uncertain about how much security was needed and how to justify what they implemented.

This is also related to some other notions and definitions of "system" and "ownership" and "responsibility" and "due care." Questions included: What is a system?; Is it the hardware or the software or the data or the communications?; What is ownership?; What does ownership imply or entail?; and What are the limits of responsibility?

Although the message about the need for standard definitions relating to "sensitive" was clear, interviewees differed with respect to the organizational level (i.e., federal, agency, organization unit) at which this should be done. Many felt levels of sensitivity (and corresponding protections) are a function of the specific agency mission and environment.

Some issues identified in the interviews as directly related to the definitions of "system" and "sensitive" are: 1) determining appropriate controls for each defined system, and 2) certifying a system is adequately protected (including selecting a basis for certification). One interview group wanted to see a "system security features minimal requirements list" for each level of "sensitive system" in each of the general support and major applications system categories. (See discussion on certification and minimum protections in Section C.3.b. Also see Appendix I for a description of the NIST minimum security requirements document.)

C.2.g Users Want to Know How to Securely Share/Exchange Data and Resources with Other Agencies and with Industry. A Few also Want Help in Dealing with Vendors and Contractors

Issues concerning sharing of information and resources are closely tied to

concerns expressed about definitions of the terms "sensitive" and "system." Instances of such sharing among government entities and other institutions are increasing. A number of interviewees spoke about system definition and responsibility issues which arise when a system interacts with entities outside of the system's physical, logical, or organizational boundaries. Specific problem areas are computers used for telecommunications, networked computers, and systems that utilize contractor support or facilities. Determining the boundaries of security responsibility for a mainframe complex running several applications or very large applications that encompass diverse hardware and sub-applications is also difficult. The study working group felt there is a need for agencies which share data or resources to have a way to determine the security for that data and resources are appropriate and adequate. (See NISTIR 4409 on the Computer Security and Privacy Plans Review Project for a further discussion of system aggregation, system boundaries, telecommunications and networking, system interfaces, and contractors.)

Some of those interviewed were in situations in which they are required/directed to use another agencies' facilities. They were seeking help in formulating questions the supporting facilities must answer regarding responsibilities and protections. Some interviewees expressed a need for security standards among agencies who share information. The standards should ensure uniform handling of information. They suggested a standard is needed regarding the handling of data by the receiving agency. Data-sharing agreements are primarily addressed with memorandums of understanding between the parties. (See the Computer Matching and Privacy Act regarding some aspects of the sharing of agency data.)

Only 25 percent of the respondents rated developing a personnel security program as *highly important* or *very highly important*. However, a small amount of interest was expressed in the interviews in guidance to train and bring contractors and other third parties "up to speed" regarding different security environments and the need to greatly speed the background investigations required for employee and contractor personnel security clearances.

Dealing with vendors was raised in a number of interviews and in remarks by survey respondents. Some indicated it was hard to get industry's attention. They saw a need for establishing liaisons with the vendor community and in pooling requirements to motivate vendors to respond to current and projected requirements. They also wanted to know what products vendors were planning and what protections would be incorporated in those products.

C.2.h Many Want to Know How to Address Security Throughout the System Development Life Cycle

The need for early emphasis on security in the system development life cycle was expressed by many. A related need was fourth among the candidate needs rated in the survey (with 44 percent calling such need *highly* or *very highly important*). The importance of needs in this area was also indicated in the interviews, with the difficulty and cost of retrofitting security after a system is in place being noted. Many of those interviewed saw a need for tools and guidance on the role of each player in building security into the system at the earliest stages was requested. (See NIST SP 800-4, Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials, for a discussion of computer security considerations in federal procurements and NIST SP 500-153, Guide to Auditing Controls and Security: A System Development Life Cycle Approach, regarding life cycle security considerations.)

C.3 Issues Concerning Basic Security Functions and Activities

C.3.a The Need for Tools and Guidance Regarding Risk Management Ranked High

The candidate need that explicitly identified risk analysis was ranked 10th in importance by survey respondents. Additionally, many related needs were expressed in the interviews and in the additional comments by survey respondents. These included the need for better understanding of all aspects of risk analysis and its role in the whole risk management process. Also identified was the need for guidance and tools for specific activities within the process. It was noted by a number of interviewees that these tools should be flexible to be easily applied to their environment and not be more complex than is absolutely necessary to adequately address the problem. Some of those interviewed indicated they had developed manual and automated tools they would be willing to share with others.

C.3.b In Protecting Sensitive Systems, Users Want to Know What is Expected, Appropriate, and Adequate

Although the survey candidate need that explicitly addressed certification did not

get a high importance score (only 29 percent of the respondents rated it *highly* or *very highly important*), related needs were more strongly expressed in the interviews. Issues concerning "what is expected?", "what is appropriate?", and "what is good enough?" were echoed a number of times. They wanted consistent rules everybody played by, so auditors know what to look for and users know what to do. Meaningful checklists, something analogous to an Underwriter's Laboratory (UL) seal or NSA's "Orange Book" evaluation process for products, were sought by those interviewed. A government standard for the certification and accreditation of systems and networks were offered as a way to address this set of needs. The standard would be spelled out in terms of step 1, step 2, step 3 and would include who or what level signs off and a NIST *"stamp of approval"* on products and procedures to protect sensitive systems.

A number of those interviewed indicated it would be extremely useful if NIST clearly defined minimum standards of what is acceptable. They felt too many of the areas appear to be subject to interpretation. They wanted the standards to be clear and "real world," and they felt examples and references to current environments (e.g., LANs, WANs) would be of value.

Some of those interviewed said help is also needed in performing independent conformance reviews. They indicated guidance on what to look for in such reviews, and guidance on how to verify that controls (e.g., those described in a security plan) are in place and adequate, would be of value.

C.3.c Contingency Planning, Disaster Recovery, and Backups Were Identified as Significant by Survey Respondents

The area of contingency planning and disaster recovery was fifth among the candidate needs rated by survey respondents. Forty-six percent rated this area as being either *highly* or *very highly* important. Although the subject did not come up often in the interviews, those that did raise the subject indicated it is important to them. Checklists, fill-in-the-blanks, and *"reasonable"* guidance that took into account the size and complexity of the system were identified as being needed. Related guidance applicable to LANs and distributed and remote systems were also desired. As with other areas of identified needs, those interviewed wanted to know what others are doing in this area.

C.4 Issues Concerning Security Awareness and Training

C.4.a There is Strong Support for Security Awareness and Training. Needed are Realistic and Meaningful Requirements and Guidance, Training, and Materials Geared to "Real World" Circumstances.

The importance of security awareness and training (SA&T) was one of the major themes of the interviews and in comments included in the surveys. Additionally, SA&T ranked just below the top third in terms of importance of candidate needs.

SA&T issues raised in the interviews include: general and specific understanding of the training problems; identifying, understanding, and evaluating potential solutions; finding resources (i.e., sources of training, training aids, and materials); and implementing solutions. Many interviewees saw a need to determine the correct level at which to apply related policy, guidance, training, tools, materials, or assistance.

Most of those interviewed saw value in and strongly supported the principle of SA&T. However, some interviewees expressed concern and frustration that current training requirements frequently offered little correlation between the training requirements and what the user needed to know to perform his or her job. They reported current requirements encourage a look at "numbers" and *"box checking"* (such as the number of hours or courses, or whether a particular film was viewed) rather than at the quality and relevancy of the training. Interviewees wanted consistent and realistic SA&T requirements expressed in terms of goals and ends rather than in terms of means or subjects to be taught. It was acknowledged that the distinction between "learning objective" and "course content" can be difficult to make.

There was wide agreement on the need for tools and materials to help with SA&T. There was also general consensus that the tools should be designed to be flexible for maximum tailoring by the agency so they could be geared to the specific situation. Some felt those closest to the situation were in the best position to know what was needed. Others thought general training (awareness & agency policies and procedures) needs to be conducted at the agency level.

Many of those interviewed expressed a need for security training. A number of them indicated they saw a void in the training available on protection sensitive, unclassified systems (analogous to the ones provided by NSA for classified data and systems). Many looked to NIST to do such training or assist in establishing a

course that would be geared toward their needs. Among the types of education, training, or help interviewees thought NIST could provide were: executive-level class on information security; specific education on useful topics; and resources to answer questions (e.g., who should accredit systems?)

Funding for training did not appear to be an issue for some, although the funding issue was not pursued.

Many of the groups indicated they are always looking for new approaches to security awareness and training. One of the potential ways to raise awareness about security within the IT community identified in the interviews was to have "credentials" established for security professionals. Also, there was the strong desire to know what others are doing and to share where practical. As an example of the potential of such sharing, the exchange of information currently taking place regarding training authoring systems was given. (See NIST SP 500-172, Computer Security Guidelines, for information concerning training areas and audience categories. Also see the NISTIR 4846, Computer Security Training and Awareness Course Compendium and Appendix K for a description of the FISSEA Develop-a-Curriculum (DACUM) effort.)

C.4.b Executive-level Security Awareness and Training Are Viewed as Critical to Obtaining Top Management Support

One of the areas of needs ranked particularly high (seventh among rated candidate needs) related to executive and management SA&T. This was strongly echoed by the interviewees who felt this was needed because of the role, model, and message executives and managers presented to the rest of the organization. It was also very important because these were people who are making the resource and budget decisions that affect the organization's security program. (See Section C.2.a for a discussion regarding justifying security resources and Section C.2.b for a discussion about addressing security in an environment of competing (production and other) demands.)

C.5 Issues Regarding Technical Approaches, Methodologies, and Products Dealing with Security

C.5.a Help is Strongly Needed with Technical Approaches to Satisfy Security Objectives. Help Must Be Simple, Cheap, Practical, and "Real World"

There was a clear message from the surveys and interviews that technical help with regard to security is sorely needed. (See Section C.1.a for overall survey results.) However, repeatedly, the study team heard the themes of cheap, practical, "real world," simple, reliable, easy to use in terms of the technical help they wanted. People don't want to have to *"struggle"* to get their jobs done.

Many people said the scale of any security activity should be responsive and appropriate -*"there are grades of everything"* - e.g., mini plans. Some interviewees saw simple tools and guidance as a means to avoid having to go to a contractor, based on the unnecessary complexity of an security task needed to be done or tool needed to be used. Some also felt when guidance and tools are small and simple, it is easier to understand, tailor, and share them.

C.5.b Help is Sorely Needed in Applying Security in LANs, Networks, and Open Systems, and to Workstations and PCs found in these Environments

Needs related to LANs got the highest rating of importance among the candidate needs in the survey. Approximately two-thirds of those responding said needs in this area were either *highly* or *very highly important*. Strong needs in this area were also voiced in the interviews. It was felt new guidance and tools must take into consideration that *"nearly everything is networked."*

Candidate needs related linking PCs, LANs, and mainframes ranked second highest among the responses in the survey (with 61 percent indicating it was *highly* or *very highly important*). It is taken as given PCs are integral to our use of IT. This message was emphasized in the discussions with the interview groups.

A resounding message from respondents and interviewees was that since these new environments were an everyday reality, they wanted guidance and tools to know what protections are adequate and appropriate and how to perform basic security functions (e.g., risk analysis and contingency planning and disaster recovery). A number of interviewees were looking for product-specific and environment-specific technical information and technical approaches. Many were looking to NIST to tell them what was necessary to do.

Interestingly, guidance on integrating open systems ranked in the top third of needs among all respondents and even higher, sixth, among GS/GM 15s and SESs.

C.5.c There was Some Interest in Having an Emergency Response Capability

None of the survey questions explicitly mentioned viruses. However, two candidate needs addressed emergency response capability, which is a way some organizations address virus attacks. Forty-two percent of the respondents thought the need for a policy related to having an emergency response capability (A07) was *highly important* or *very highly important* and rated this need 16th. Thirty percent of the respondents thought the need for guidance and assistance related to having an emergency response capability (B05) was *highly important* or *very highly important* and rated this need 30th.

During the course of the interviews, and from respondent comments, a number of issues were raised with respect to viruses and emergency or incident response. The following is a sampling of them:

- Need for operational or policy guidelines the users or system administrators can follow, including installing system patches.
- Need for a national level incident response.
- A number of interviewees expressed concern about the potential for Unix viruses. They said guidance and products may be needed in the near term.
- Need for a constant upgrade of virus scanners to filter out suspicious code that will likely appear. Need to look at issues of re-infection and false alarms.
- Need virus protection software for all machines.
- Need guidance on how to prevent employees from importing personal virus-infected diskettes.
- Need for distinguishing technical and administrative approaches to virus protection and to pursue both.
- Need for protecting software across open systems from corruption due to viruses.

Some knowledge, but not a lot, was expressed regarding the Forum of Incident Response and Security Teams (FIRST). (See Appendix Z for additional information.)

C.5.d Significant Interest was Expressed in Security of Databases, Distributed Data, and Distributed Processing

Database security ranked very high (third) among survey respondents. Issues concerning the protection of distributed data and distributed processing

capabilities were also important to many of those interviewed.

Some of the related issues or needs identified included:

- Need guidance on what to do about the physical distribution of the database (including all the data on PC floppies).
- Need guidance on the monitoring of IT resources in light of the potential access by one individual to huge repositories of information from many agencies.
- Need guidance on categorization and labelling.
- Need guidance on how to administer security in a decentralized environment.
- Need guidance on uploading/downloading between PCs and mainframes.
- Need guidance and policy for maintaining data integrity in a cooperative processing environment.

Interviewee concern was expressed that the whole area of distributed processing and distributed responsibility was filled with many unexplored and unimagined potential problems. As one interviewee said, *"We don't know what we don't know."* (See Appendix I for a description of the NIST Integrated OIS, ISDN, and Security Program for related information. Also see Section C.4.b on LANs, networks, and OSI.)

C.5.e There was Some Interest in Products and Tools to Control Access

This category rated relatively low among the survey candidate needs (with only 31 percent rating it *highly* or *very highly important*). However, the issue of access control was communicated more strongly in the interviews.

Some interviewees were looking for tools and products for access control, but were also concerned that the particular method used be workable in their environment and with their users, customers, and clients. Some looked to combinations of biometrics and secure ID tokens as possibilities. Most seemed to be looking beyond simple passwords and were looking for solutions incorporated into products.

C.5.f There was Moderate Interest in Identification, Authentication, and Encryption and Some Confusion about Alternatives

A number of those interviewed expressed interest in getting help in these areas. The candidate need covering access control and authentication (need C01) was 29th among rated needs, with 31 percent of respondents rating this need *highly important* or *very highly important*. The candidate need addressing electronic data interchange, public key encryption, digital signatures, and electronic authentication (need C07) was 17th among rated needs, with 35 percent of respondents rating this need *highly important* or *very highly important*.

In general, interviewees were unclear about what they were required to use or do, what options were available, how to evaluate among alternatives, what products and technologies were approved and by whom, and how to build in these technologies as part of the system development process. They were interested in not only what would work and provide the desired degree of protection, but also what would stand up against scrutiny and challenge. Cost of implementation and operation was a major issue to many of those interviewed who had a need for application of these technologies. Another consideration was ease of use and convenience, especially in high volume production environments.

C.5.g Need for Products and Systems Satisfying National/International Criteria for Protection Rate Low in the Survey Compared to Other Needs

Needs in the survey that directly addressed national and international criteria ranked the lowest among the rated candidate needs, with only 14 percent of the respondents identifying this need as highly or very highly important. However, there was interest expressed for this area and for trusted systems during the interviews. There was one area of national and international criteria that did generate interest in the interviews. This area was in regards to the minimum security requirements for systems and the ability to buy commercial off-the-shelf (COTS) products that incorporate these security features.

The study working group felt the low ranking may have been due, in part, to the fact the survey wording did not clearly express the intent of this need. It was felt a revised statement of the candidate need may have produced a truer assessment of its importance. What follows are the original wording of the candidate need and a rewording that might have avoided some possible confusion:

Original version as it appeared in the agency security needs study:

"[PR], [S] satisfying national/international criteria"

(Further Description: *"Products and systems satisfying national/international criteria for protection of data and systems and that address integrity and availability in addition to confidentiality"*)

Potentially clearer version:

"[PR], [S], [TA] for trusted technology that consider a wider range of functionality appropriate for unclassified, sensitive systems than now covered in NSA's TCSEC ("Orange Book"), and which satisfy national/international "criteria""

(Further Description: *"Products, standards, and technical assistance for trusted technology that consider a wider range of functionality appropriate for unclassified, sensitive systems than now covered in NSA's Trusted Computer Systems Evaluation Criteria, "Orange Book," (i.e., for protections of data and systems that more directly address integrity and availability in addition to confidentiality), and which satisfy national/international "criteria." International computer security criteria is used to develop trusted IT products that can be used to help protect important information of the government, whether it is sensitive or classified. This type of criteria helps to broaden the market for these products making them more available to potential buyers. International criteria also increases the number of COTS products available for various computer security needs."*)

C.6 Issues Concerning to Security Information and Sources of Help

C.6.a There is Lack of Awareness of Available Sources of Help

The study team found lack of awareness of available help and resources to be a major issue. It is an area that represents lost or untapped potential for federal agencies.

While clearly there are not existing answers to many of the needs expressed, the study team came across many situations in which those interviewed were not aware of existing solutions, products, and answers. This was especially true regarding awareness of many of NIST's documents and services.

The study team found the study participants had a great hunger for information. This phenomenon manifested itself in the survey responses and in the interviews. Respondents and interviewees wanted to know what others are doing, how they

are addressing particular issues and problems, and what products, documents, tools, procedures, and studies others have that could be made available. The study team was heartened that many such things are available and that the producing agencies are eager to share what they have.

Some of the interviewees were not fully familiar with a number of existing resources regarding available help and for knowing what others are doing. These resources include the Federal Computer Security Program Managers' Forum, the NIST Computer Security BBS, the NIST Security Clearinghouse, and such meetings and conferences as the NIST/NSA co-sponsored National Computer Security Conference. (See Appendix I and Appendix H for descriptions of these activities.)

C.6.b *A Clearinghouse and the Free Flow of Information about Security* Are Wanted

One of the loudest messages heard in the interviews and comments of respondents concerns security needs and desires related to the flow of information. The message was not expressed as loudly in the survey responses, with the candidate need explicitly addressing the clearinghouse function being ranked in the middle third in terms of importance and only 36 percent of the respondents rated this either *highly* or *very highly important*. However, related needs were expressed in many forms.

Interviewees indicated they see a clearinghouse as more than a collection of and repository for information - although it certainly is that. It is also a concept and way of looking at the needs of the community it is serving. It is also a collection of activities and services. Some saw the clearinghouse as potentially part of a very proactive federal role with regard to getting maximum "bang for the buck" in terms of work already done. They also saw it being used to stimulate security-related activity. Another possible role for the clearinghouse was in identifying the "holes" in a federal security master plan.

A number of respondents and interviewees said they would like to see models or examples of things they needed to do or produce. Agency policies, procedures, computer security programs, training modules, security plans, contingency and disaster recovery plans were among the things identified.

Although not raised as a major issue, there was discussion in the interviews regarding the form of the information being shared or accessed. There seemed to be a general consensus that electronic form was better than non-electronic and friendly, easy, quick retrieval improved the system's potential use.

Interviewees did not necessarily care where the clearinghouse resided or that it resided in only one place. However, many of those interviewed saw NIST playing an important role in this area. (See Appendix I for a description of the NIST Computer Security Interagency Information Center and Appendix I for a description of the NIST Computer Security BBS.)

C.7 Study Participants See NIST as a Key Player in Addressing their Security Needs

Although only one question in the survey explicitly addressed NIST's role (i.e., need D02, better flow of information from NIST to its constituency), nearly all of the other survey candidate needs implicitly addressed this issue. There was consensus that NIST should play a key role in helping agencies address their security requirements. There was also general agreement that NIST's role in security ought to be further clarified.

Two issues came up with respect to NIST providing help to its constituency. One issue was that NIST publications and documents exist that might be of help, but the users are unaware of them. (See above discussion on the lack of awareness of available help resources.) The other issue concerns NIST publications and documents that exist and cover the general subject area, but are not adequate (perhaps because of quality, level of specificity, currency) for the user's problem. Interviewees felt both issues need to be addressed.

Support for an expanded NIST role was voiced. Many want to see NIST be more proactive, reduce time in getting new or revised standards out and ensure the user community is informed of these changes. They wanted NIST to provide useful, meaningful help. They also wanted NIST to have the authority and they wanted to see more situations where NIST gives its "stamp of approval." NIST's security efforts are respected by those interviewed, despite recognition of constraints of NIST budget limitations.

SECTION V.
CONCLUSIONS

A. Overview of Conclusions

The conclusions made in this section are based on the agency needs survey and interviews and on discussions among the study team, the TARs, the study working group, and NIST staff. The study working group has indicated the needs expressed in this report are consistent with the data presented and with their experience and understanding of the federal security environment.

It should be noted the study did not find security needs that were "*unimportant.*" It appears to the study team that assistance in any of the need areas identified would be of value to at least some of the study participants. However, taken as a whole, some needs were clearly identified as more important to the participants than others. A full appreciation by study participants of all of the candidate needs listed in the survey may have to wait for more universal and in-depth awareness and understanding of security issues and technology.

Section B.1 addresses the needs for specific technical guidance documents on a variety of subjects as directly expressed in the agency needs survey and confirmed by the interviews and discussions with the TARs, the study working group, and with others. While some of the needs in the other sections below also derive directly from the survey, for the most part, Sections B.2.a through B.2.g address needs gleaned from analysis and discussions, and include needs in the area of security management (including resources), policy, access to information and security awareness and training (especially with regard to executive management), and knowing what security requirements will be imposed and the type of help that will be needed and that can be anticipated. Section C speaks to the need for further validation of the study and continuing assessment of security needs. Looked at another way, Section B.1 covers needs describing the *"what,"* i.e., the technical security help being sought, and Sections B.2.a through B.2.g cover the *"how"* or the processes that could facilitate that help. Section C covers the outcome and follow-on activities to the study itself. Section D talks about NIST actions that support agency security needs. Section E presents some final thoughts.

B. Conclusions Regarding Needs

B.1 Need for Specific Technical Guidance Documents

B.1.a There is a Need for New NIST Technical Guidance Documents and for a Major Revision/Update of Existing Documents

The study team found a clear need for a major revision and update of a number of the NIST FIPS pubs and related technical guidance documents, as well as the need for new documents. The following areas were explicitly identified in the survey (i.e., ranked among or near the top third) as requiring attention. Their importance to study participants was echoed in the interviews and affirmed by the study working group. (Respective rankings and survey need number are given in parentheses.)

Specific technical environments needing attention:

- LANs (rank 1, need C10)
- integration of PCs, LANs, and mainframes in one security architecture (rank 2, need C11)
- database security (rank 3, need C14)
- secure dial-in and laptops (rank 6, need C13)
- integration of open system environment products (rank 11, need C12)

Policy, management, and technical areas and basic security functions needing attention:

- security in the system development life cycle (rank 4, need A05)
- contingency and disaster recovery planning (rank 5, need B02)
- defining and protecting sensitive systems (rank 8, need A09)
- developing security plans (rank 9, need A10)
- risk analysis (rank 10, need B01)
- information collection, dissemination, and sharing (rank 12, need A06)

(Note: Policy, guidance, and training promoting security policy awareness among executive level functional and technical managers (rank 7, need A03) and guidance, products, assistance, and materials for security awareness and training (rank 14, need B09) are addressed in Section A.4, below. Policy and guidance on integrating security policies and directives (rank 13, need A01) is addressed below in Section A.2. Needs related to a clearinghouse of security information

(rank 15, need D01) are addressed in Section A.4.)

Among the types of documents needed is a series of "how to" documents. These would explain to the reader how to use the updated, revised, and new policies, standards, and guidelines, referred to above. These documents would emphasize the interpretive nature of the updated, revised, and new policies, standards, and guidelines. They would show how to apply the policies, standards, and guidelines in different environments and clarify the "enforceability" (i.e., mandatory or optional) aspects of each document.

As indicated in Section IV, emphasis of any guidance documents must be on help that is simple, cheap, practical, and "real world."

B.2 Needs Related to IT Security Management, Policy, Training and Information

B.2.a There is a Need to Help Agencies Develop Fully Robust and Integrated Security Programs

While not specifically addressed as such in the survey, it appears to the study team that agencies need help in developing fully robust and integrated security programs. Such a program is more than a collection of computer security and privacy plans prepared in accordance with OMB Bulletin 90-08. It includes the full range of technical policies and procedures and the implementation of cost-effective, risk-based controls that are addressed starting with the system development life cycle. Needed in this area are commonly agreed upon definitions of "system," "sensitive," and "adequate protection." Also needed are consistent and integrated federal IT management directives to ensure they appropriately reflect security considerations. These would include federal policy integrating security, IRM, personnel, acquisition, internal controls, and financial management. (See Sections IV.C.2.d and IV.C.2.h.)

B.2.b There is a Need for More Federal and Agency Security Resources and a Need to Better Effectively Use and Leverage Resources

As indicated in Section IV, a frequently heard theme was there were not enough security resources to do the job the way those who had direct responsibility for security would like to do it. This translates into a need for additional resources, a way to better leverage existing resources, or both. (See Section IV.C.2.a)

B.2.c There is a Need to Access Relevant Information and a Need to More Effectively Share Information Regarding Security

One way to leverage resources is to get at and share information. The study and study working group found a strong need for a national state-of-the-art clearinghouse of all public domain security documents and publications. This would include policies, procedures, guidelines, manuals, models, and tools either produced for governmentwide or agency-specific use. The study working group felt strongly this would require a high visibility, proactive leadership role and committed participation by the entire federal community. It was felt the continued growth of the NIST computer security BBS and the NIST Computer Security Interagency Information Center (CSIISC) clearinghouse were steps in that direction. (See Appendix I.)

There is a strong need to find more structured ways in which to facilitate cooperative efforts among agencies to share knowledge, experience, and documents developed by federal agencies. Study participants thought a federal organization might provide leadership in this area.

The study working group encouraged the use of special focused workgroups to collaboratively address the updates, revisions, and new documents. The study working group reported a willingness on the part of the federal security community to participate in such efforts. The study working group saw this as a way to leverage limited resources and a way to bring vital, additional "real world" experience to bear. It has been suggested that existing federal organizations, such as the Federal Computer Security Program Managers' Forum, might provide leadership for such activities.

The study working group saw potential value in establishing an electronic group decision support system (GDSS) center that could be used to more effectively facilitate group-developed guidance documents and training tools in the area of IT security. The center could be used as a general federal resource to support other federal (interagency and intra-agency) group decision-making processes. (See Appendix K for a description of FISSEA DACUM effort.) (See Section IV.C.6)

B.2.d There is a Need for Guidance, Assistance, and for Authoritative Information Regarding Security

There was general agreement on the need for, and value of, guidance and assistance in the technical and non-technical areas of security. There was also

a related need for an "authoritative" source for information regarding security policy and the application of security technology. Some pointed to the National Computer Security Center's use of "desk officers" as a possible model. Others saw value in a "help desk" or a 1-800 or even 1-900 telephone number to provide the desired help. (See Section IV.C.1.d.)

B.2.e There is a Lack of Consensus Regarding the Need for Stronger Federal and Agency Security Policy

Some study participants wanted to see both governmentwide and agencywide enforcement language and mechanisms to put "teeth" into security policy. Such policy statements, directives, and procedures would provide clear statements or roles and responsibilities regarding security. Some felt requiring the inclusion of security-related elements in individual performance plans would be useful. There were others, however, who felt very strongly that establishing additional security requirements through federal directives was unnecessary and could be counter-productive. They felt current policy is adequate and any additional requirements should be internally generated. What was needed was help in doing what they knew had to be done. (See Section IV.C.2.e.)

B.2.f There is a Need to Raise the Level of Security Awareness of Agency Management and Raise the Stature of Security Practitioners

There was concern among interviewees regarding the awareness of security issues and concerns by executives, functional managers, and information resource managers. It was felt lack of awareness made it extremely difficult to communicate with them about security and for security to effectively compete for resources with other management concerns. The study working group identified the need for a federal organization to provide leadership and tools to assist agencies by: 1) providing them with security awareness materials; and 2) developing security training materials suitable for a variety of audiences, with particular priority placed on materials geared to executives and functional managers. The study working group thought this was an appropriate role for NIST.

It appears that in many organizations, security continues to be an "additional duty." The study working group felt that establishing a separate job series for security professionals would raise management awareness about the importance of security. The study working group also felt strongly the security function should be separated organizationally from operations. This was thought necessary to avoid undue influence under work situation pressures. It was also felt steps

leading to the professionalization of security practitioners was a good thing. (See Section IV.C.4)

B.2.g There is a Need to Better Anticipate Security Requirements and Needs and Better Anticipate What Kinds and Forms of Support Will be Available

Agencies need to do a better job anticipating their security requirements and needs. Vendors would be better able to respond to changing government security repuirements, if these needs are more effectively communicated. This process could be helped if federal planners provided information about long range strategic directions. Also helpful would be stronger federal liaisons with the vendor community so the availability of vendor products will be "in sync" with near-term and long-term federal security needs.

The study working group felt that there was a need for some organization to work with the vendor community to encourage the development of a security "architecture" and products that support the architecture. The architecture would permit the development of IT and security products that could function in a variety of environments, including multi-vendor distributed processing. (See Section IV.C.1.a)

In an attempt to anticipate and respond to future needs, a number of national and international efforts are underway aimed at developing criteria and evaluation processes. These efforts are directed toward systems providing single level and multilevel security. (See Appendix I for a discussion of criteria-related efforts.)

C. Further Validation of Study Results

The study working group echoed a message voiced at the beginning and heard throughout the study - i.e., the security needs determined in this study should be further validated among the community through discussions with a variety of audiences. Further, they felt there is a need to periodically update the picture of federal security needs developed in this study and to assess progress in addressing those needs.

D. NIST Activities that Support Agency Needs

A number of current NIST efforts directly or indirectly address the collection of needs expressed in the survey, particularly the ones that were among those indicated to be more important. (See Appendices H, I, and J for additional details and for some sources of information for those who are determining security needs or looking for help in addressing those needs)

It is expected NIST will be further developing ongoing communications channels. This may involve: maintaining regular liaisons with key federal groups (e.g., President's Council on Integrity and Efficiency (PCIE), Federal Computer Security Program Managers' Forum (FCSPMF), Federal Information Resources Manager's Policy and Oversight Committee (FIRMPOC), Federal Data Center Managers Council (FDCMC); Federal Information Systems Security Educators' Association (FISSEA), and private sector organizations. It is also expected NIST will be further developing informal communications channels (e.g., electronic mail forum(s), NIST Computer Security Bulletin Board System (BBS), and other BBSs), and maintaining ongoing agency interactions, including representing NIST on security-related working groups and steering committees. (See Appendix H.)

E. Some Final Thoughts

Those organizations the study team worked with and visited appear to have a deep commitment to security, despite a number of constraints, limitations, and frustrations. They are looking for a clear statement of what is required and expected of them with regard to security - and they expect these requirements to make sense and to be consistent with their other requirements. In simple terms, they are basically saying, "Give us a clear statement of what is expected of us. Give us resources to do the job. Provide us support and assistance in doing the job. And we'll get the job done."

While agencies regard NIST as one important source for help, they are not standing idly by. They are developing programs that work for them. They are also beginning to coordinate their efforts with other agencies. There is clearly a need for federal agencies to continue to be proactive with regard to IT security and define the role that they need to assume in their own behalf. In this regard, it is recommended federal agencies continue to monitor their security needs, communicate these needs to the central agencies, seek sources of help from within the federal community, and be generous in the sharing of their own experiences and products.

It was clear from the September 1992 study working group meeting and from discussions with the target agency staff and TARs that the security community wants to know what help they can expect with their security needs. They want to know what NIST itself will do, what NIST will do to facilitate the projects of others, what NIST understands other agencies will do, and what NIST understands agencies will do for themselves. NIST is committed to using the results of this study as input to its planning process and to communicating that through its annual report, its security program strategic plan, and through other forums. NIST is also committed to communicating the study results to others as appropriate.

Finally, this study is but one piece of a much larger mosaic. We believe this project is an important element in providing a sound basis for planning future NIST security-related efforts. In addition to NIST and the other central agencies, each agency, its security staff and structure, and individual users are among those that play an integral role in providing comprehensive security for the federal government. In deciding where to apply resources and energies, it is important to take into account the roles and relationships among all these players. There is an open invitation and welcome for all to join in the search for and development of solutions that serve our community.

LIST OF APPENDICES

APPENDIX A
FIRMPOC SURVEY AND RESULTS

The following are the information technology (IT) security needs expressed in response to a questionnaire distributed to the members of the Federal Information Resources Manager's Policy and Oversight Committee (FIRMPOC). These responses were used as one of the bases for the agency IT security needs assessment survey.

The FIRMPOC questionnaire presented the respondent with a set of open-ended questions, including the following:

- What problems do you think NIST should be solving?
- What specific information security standards or guidance do you think that NIST needs to develop?
- What additional specific information security-related services do you think that NIST needs to develop?

The responses are presented below with one or more keywords, subjectively determined by the study team. Each keyword or set of keywords is followed by the related needs expressed in the FIRMPOC responses.

KEYWORDS DERIVED FORM THE FIRMPOC SURVEY

access authorization, access control

Access authorization and control

How to integrate manual controls, software, and physical controls to achieve reliable, effective access control

Identify techniques and products which supplement passwords (i.e., highly reliable, cost-effective tools to protect sensitive data from unauthorized access)

agency needs, coordination, and communications

NIST should continue to periodically survey independent agencies through the Federal Computer Security Program Managers' Forum and other organizations

authentication, digital signatures

Authentication, digital signatures

automated information, legal admissibility

Guidance on practices regarding legal admissibility of automated information (text, image, etc.)

budgets, security management, contingency planning

Funding of organization-wide central contingency planning, including implementation, testing, and follow-up, controlled at the administration level

Separate agency budgets for AIS security

business problems, business solutions

Assistance in obtaining (user-oriented) solutions to business problems targeted to the federal community, not as technical as those required by the scientific community - industry product marketing brochures are an example - could be used for getting federal comments

certification, accreditation, system development

Certification and accreditation procedures should be standards rather than guidelines - so as to ensure inclusion in the system development process

Lack of certification of applications

CERTs, incident response, contingency planning authentication and verification, electronic signatures

Specific guidance, similar to FIPS 87 - contingency planning, related to setting up a CERT to anticipate and address specific emergencies

clearinghouse, product reviews

NIST should provide a clearinghouse for agency-developed computer security policies and guidelines, in electronic form categorization, using CSA categories for sensitivity

Clearinghouse of experience with computer security wares (hardware and software)

computer criminals

Establish guidance on the prosecution of computer criminals

computer network security

Computer network security

Importance of computer/network security as "only management control factor" capable of assuring C,I,A for our government

computer security awareness and training, minimum training requirements

Mandatory minimum security training requirements

Expand the IRM security awareness campaign

computer security needs, computer security policy

Effort to identify and prioritize needs is good - need for strong national

oversight for OMB/NIST/NSA - Congress needs to be kept informed

computer security planning
"Nuts and bolts" guide to ADP security planning and preparing security plans

computer security policy, computer security management security
OMB/NIST/NSA should work together to explore the identification and development of mechanisms to determine feasibility of national computer security implementation initiatives so agencies can better understand and prioritize their actions

contingency planning
AIS contingency planning

contingency planning
Contingency planning

contingency planning, disaster recovery
Contingency planning, disaster recovery

criteria, sensitivity levels, evaluation
Criteria for evaluating sensitivity levels

cryptographic security measures
Determining when and how sensitive information must be protected with cryptographic security measures - law mandating protection, especially for exchanges with the public

cryptography
Cryptography

data categorization
NIST should develop policies and guidelines regarding data categorization, using CSA categories for sensitivity

database management security
Database management security

DES, export controls, international standards
Ability to exchange encrypted information on an international basis - new DES standards not subject to export controls

electron authentication and verification, electronic signatures
FIPS PUB on document authentication and verification, a logical extension to project to establish electronic signature standard

electronic FAX
FAX machines

electronic forms
Problems with making electronic forms a reality

electronic mail security

Electronic mail security

electronic signature, legal aspects

Agreement between legal community and computing community on electronic signatures

Electronic signatures

emergency response teams

Emergency response teams

evaluation, certification, encryption, authentication

A formal NIST evaluation/certification program for encryption/authentication techniques or devices for sensitive, but unclassified data for civil agencies

Adoption of a simple governmentwide procedure for evaluating and certifying controls

federal criteria, trusted systems

Federal Criteria for Trusted Systems

Use FCSPMF to support policy and guidelines through workshops and group participation

NIST should expedite work with NSA to develop criteria that reflect civilian concerns (including integrity and availability) to lead to low cost COTS security and accredited products to compete worldwide

Civilian LAN and WAN security standards, and maybe revise and adapt DoD's Trusted Network Criteria, leading to COTS tested and accredited products to compete worldwide

federal regulation, computer security management and planning

Briefing on status of revising OMB Cir A-130

OMB/NIST/NSA coordination to expedite rev of OMB Cir A-130 - as national umbrella policy for AIS classified/unclassified security, to include a clear national requirement related to incident response capability, periodic on-site security reviews, use of encryption to protect sensitive/critical data, and others

federal regulations, new technologies

Expedite update of OMB Cir A-130 to reflect new processing capabilities and technologies, with priority on distributed processing, electronic facsimile, record keeping, archiving, and LANs)

Expedite update of OMB Cir A-130 to reflect new processing capabilities and technologies, with priority on distributed processing, electronic facsimile, record keeping, archiving, and lans)

NIST should develop and revise standards and guidance iaw new A-130

FIPS, updating, current technology and industry practices

Revise FIPS to conform with current technology and industry practices (micro, mini, mainframe, distributed environments, communications, etc), especially FIPS 31, 65, 87, 102

general computer security

Additional help is needed in security

GOSIP, POSIX, SDNS

NIST should develop integrated telecommunications and computer security program guidance, building on FIPS 146-1, GOSIP standards documents, especially FIPS 65 (risk analysis), FIPS 87 (contingency planning), and FIPS 102 (certification and accreditation)

Authentication protocols developed and included in the GOSIP suites

Briefing on the importance of integrating security into POSIX and GOSIP standards - and increased importance of new technical security features

GOSIP standards which ensure effective authentication of authorized users, with SDNS protocols included in the GOSIP suites asap

POSIX extensions which address integrity and authentication - NIST should provide support for the development of integrity and authentication standards

incident response, incident coordination

Briefing on the importance of agency computer/network incident response/handling capabilities - and what OMB/NIST/NSA see as effective capability at the national level

OMB, NIST, and NSA should work closely together to further develop a significant national incident coordination capability

integrity, baseline controls

Establishment of governmentwide baseline integrity/security controls for sensitive systems

LAN, WAN, network security

Local and wide area network security

Comprehensive guidance for civilian LANs

LAN security

lines of communication

Better lines of communication between those establishing direction and guidance and those having to follow the guidance

Clearer guidance to minimize different interpretations

Brief FIRMPOC on entire spectrum of government's many varied AIS security

interests

minimum security controls, requirements, criteria

An overall regulation addressing minimum security controls for specific systems should be developed and enforced

Standard for implementation of minimum AIS security in the government

Minimum standards for security of different platforms - micros, mainframes, networks

network security

Governmentwide mandatory minimum requirements policy, carrying the force of law, and requiring centralized management and oversight within each agency

Guide to network safeguards and when to use them

NIST publications need to be updated to place more emphasis on "interconnected network systems"

network security, lines of communication

Increasing importance of network security in the government

Guidelines needed on how to most effectively conduct risk assessment, penetration testing, certification, compliance auditing in network environments

Guide for conducting a network security review

Guide for building security in the network's system life cycle

Network security and contingency planning

new and emerging technologies

FIRMPOC subgroup to evaluate issues in connection with new and emerging technologies from an IRM perspective

NIST publications

FIPS List 91 needs to be a current central directory of all NIST standards and guidelines on AIS security

NIST standards and guidance

Establish 3-5 year review/updating cycle for all NIST standards and guidance

NIST standards and guidance

Update critical computer security standards documents, especially FIPS 65 (risk analysis), FIPS 87 (contingency planning), and FIPS 102 (certification and accreditation)

Open System Environments

Security standards for Open Systems Environments, including encryption of x.400 bodyparts, authentication in x.500, transaction processing, file transfer

Applicability of security measures to open systems environments presented in a way that simplifies complex terminology - perhaps with the use of pictorial guides

Open systems security

Orange Book, criteria

Orange Book replacement so vendors can supply products that meet these requirements

OSI, network security

OSI/network security

outreach, awareness, NIST programs

Agencies needs to know more about NIST's current programs

POSIX, integrity, authentication

POSIX FIPS PUB needs to be expanded to include security - integrity and authentication - should be developed in cooperation with IEEE

privacy

Laws for privacy consistent with what tax payers are willing to pay to secure their tax data

public access, electronic information

Problems associated with "public access" to automated government information

public key encryption, digital signature

Briefing on use and advantages of public key encryption with an integrated digital signature feature

Public Key Encryption and Digital Signature standards asap with a national requirement for a 5 year phased implementation

requirements, needs assessment

More useful methods of assessing and determining security requirements

risk analysis, risk management

Risk analysis, risk management

NIST certification of risk management packages iaw FIPSPUBS

security awareness and training

Security training modules developed by a number of agencies working together

Awareness and training for system developers

security controls

Minimum security controls for each sensitivity level

security in ADP acquisitions

Continued work by NIST and GSA to assure agencies identify and address

security requirements in ADP acquisitions

security management, security function, security organization

Elevate management level attention of AIS security - possibly making AIS security a function of the Secretary's office

security needs, sources of needs information

Use of department security and program officials to identify agency information security requirements, including administration/agency security officers, key field security officials, major program/ project management

security reviews

Guidance on security reviews of application programs

standards and guidance

FIRMPOC subgroup to review draft security standards and guidance to ensure NIST publications appropriately reflect IRM concerns

NIST should officially distribute draft proposals that affect security while they are under development by ISO and CCITT

Continued NIST effort on DES and GOSIP standards

trusted systems

Briefing on how trusted systems technology can be selectively applied to protect systems and meet 5 year implementation requirement

A national directive which requires trusted systems (C2 functionality) for certain categories of information where confidentiality and/or integrity are primary - with 5 year phased implementation

viruses

NIST leading a FCSMF subcommittee on IT security requirements

NIST publication "Computer Viruses from A to Z"

APPENDIX B
NIST FEDERAL AGENCY IT SECURITY NEEDS STUDY SURVEY FORM

The following is a copy of the NIST Federal Agency IT Security Needs Study survey form.

NIST FEDERAL AGENCY INFORMATION TECHNOLOGY (IT) SECURITY NEEDS STUDY SURVEY FORM

May 1992

Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

DRAFT 5/1/92

SECTION I
OVERVIEW AND GENERAL INSTRUCTIONS

Dear Study Participant:

The National Institute of Standards and Technology (NIST) is chartered with helping federal agencies meet their individual information technology (IT) security requirements. It is critically important that NIST accurately understands of what agencies need to meet those requirements in order for NIST to effectively structure it's computer security program.

The effort to improve our ability to identify and assess these agency needs, initially will consist of an in-depth study, conducted by NIST and agency staff, and the establishment of on-going mechanisms to facilitate communication between NIST and agencies. We strongly believe that the information that comes out of this study can help lead to the improved protection of valuable federal information technology data and resources. Your participation in this study is a valuable contribution in that direction.

The study involves interviews with identified agency staff and the use of this survey in which respondents are asked to identify their IT security needs, from a list of candidate needs, indicating the importance and immediacy of the needs. The study will initially focus on four target agencies, selected to represent a variety of federal information technology (IT) security environments. Other organizations and individuals will be invited to participate.

In order for us to better understand your needs, please complete Section II (Identification and Environment Profile) and Section III (Information Technology Security Needs Profile). (Section IV provides a further description of the candidate IT security needs that appear in more condensed form in Section III.) Your completed survey should be returned as instructed by your agency or organization sponsor. Otherwise, please send the completed survey to:

NIST Federal Agency
IT Security Needs Study
NIST/CSL
A251 Technology
Gaithersburg, MD 20899

The needs will be summarized and documented, and reviewed at an invited workshop in September 1992. Results will be made available through a number of sources.

Please note that participation in the study is strictly voluntary, and that the study is not part of any audit or Computer Security Act (PL 100-235) security and privacy plans review effort. Requests for anonymity will be honored.

Thank you for your contribution to this effort. If you have any questions, please address them to your agency or organization sponsor, if applicable, or to Dennis Gilbert at 301-975-3872 or e-mail: gilbert@ncsl.nist.gov.

Sincerely,
The NIST Federal Agency IT
Security Needs Study Team

SECTION II
IDENTIFICATION AND ENVIRONMENT PROFILE SECTION

It would be valuable for the study team to know your perspective in understanding your information technology (IT) security needs. The following information will be helpful in that regard. All questions in this Section II are optional. *As indicated in Section I, requests for anonymity will be honored.*

I request anonymity for my survey response: Yes ___ No ___

Last Name _____ First Name _____ MI ___
Agency/Organization _____
Sub-unit _____
Position/Title _____
If federal government, grade _____
If contractor, grade equivalent _____

Street Address _____
_____
_____

City_____ State_____ Zip_____
Phone (____)_____ FAX (____)_____
E-mail _____

For each of the following lists, please place a mark next to all items that apply.

Please indicate the type of your organization:

____Aerospace
____Business Services
____Communications/Public/Other Utility
____Computers/Data Processing Services
____Computers/Data Processing Vendor
____Construction/ Mining/Agriculture
____Consulting
____Defense
____Distribution
____Education
____Entertainment
____Federal Government
____Financial/Banking
____Insurance
____Legal
____Manufacturing
____Medical
____Non-profit Services
____Research
____Retail
____State, Local, or Municipal
(_____)
____Transportation
____Wholesale
____Other
(_____)

Appendix B

If federal government, please indicate your agency:

____Dept. of Agriculture
____Dept. of Commerce
____Dept. of Energy
____Dept. of Health & Human Services
____Dept. of Housing & Urban Development
____Dept. of the Interior
____Dept. of Justice
____Dept. of Labor
____Dept. of State
____Dept. of Transportation
____Dept. of the Treasury
____Dept. of Veterans Affairs
____DoD - Air Force
____DoD - Army
____DoD - Navy
____DoD - All other
____Exec. Office of the President
____Judicial
(_____)
____Legislative
(_____)
____Environmental Protection Agency
____General Services Admin.
____Natl. Aeronautics & Space Admin.
____US Postal Service
____National Security-Related Org.
____All Other Agencies
(_____)

Please indicate your title/occupation/position/area of concern:

____Applications Programmer
____Auditor
____Business Resumption Planner
____Computer Operator
____Computer Security Officer
____Computer Security Specialist
____Computer Scientist
____Computer User
____Configuration Management Specialist
____Consultant
____Data Processing Management
____Data Processing Specialist
____Director
____Disaster Management
____EDP Auditor
____Educator
____Functional/Line Management
____Functional/Line Staff
____Industrial Security
____Information Resources Management
____Law Enforcement Officer
____Management Consultant
____Network/Communications Management
____Network/Communications Specialist
____PC Coordinator
____Quality Assurance Specialist
____Scientist
____Staff Specialist
____System Administrator
____Systems Analyst
____Systems Programmer
____Other
(_____)

Please indicate your experience in an IT security-related field:

____Less than one year
____One to three years
____Three to five years
____Five to ten years
____Ten to fifteen years
____Over fifteen years

Please indicate how you got this survey:
____From an agency/organization sponsor
(agency/organization _____
sponsor _____)
____From the NIST Computer Security Bulletin Board System (BBS)
____Directly from NIST
____Other
(_____)

SECTION III
INFORMATION TECHNOLOGY (IT) SECURITY NEEDS PROFILE

CANDIDATE IT SECURITY NEEDS TO BE RATED BASED ON THEIR IMPORTANCE AND IMMEDIACY TO YOU

Use this Section III to indicate the importance and immediacy of your needs in addressing your information technology (IT) security requirements.

In this section, each of a set of candidate needs is described in terms of one or more of the following:

Type of need:

[A]=assistance

[G]=guidance

[P]=policy (federal, other)

[PR]=products

[S]=standards (mandatory, de facto)

[T]=technology (tools, techniques, methodologies, algorithms)

[TI]=technical information, product evaluations

Next to each candidate IT security need listed below, please record one of the following codes:

Importance of the need to you:

NA = Not Applicable

L = Low or Minimal Importance - (Requirements in this area are minimal or are currently being adequately

addressed or can be adequately addressed with agency's/organization's resources)

M = Moderate Importance (Some requirements exist in this area that are not being fully addressed or it is expected that some future requirements in the area will not be able to be adequately met with the agency's/organization's resources. Some help in this area would be useful.)

H = High Importance - (Important requirements (e.g., policy, management, technical, programmatic) exist or are expected to exist and the agency//organization does not currently meet them or does not expect to be able to adequately address them in the future. Significant help is needed.)

V = Very High Importance - (Critical requirements (e.g., policy, management, technical, programmatic) exist or are expected to exist and the agency/organization does not now or does not or does not expect to be able to adequately address them. Significant help is essential.)

Immediacy of the need:

IM = Immediate - (Help in this area is needed now or within 1 year)

NT = Near Term - (Help is this area is needed in 1-3 years)

LT = Long Term - (Help is this area is needed in more than 3 years)

Ratings of Importance and Immediacy may be subjective judgments and may be based on any combination of factors that you judge appropriate to your situation.

For your convenience, the candidate IT security needs presented below are grouped into sections (III.A - III.D). The needs are not mutually exclusive - many are overlapping. Some may not apply in your environment or situation. In that case, either indicate an "NA" for Not Applicable or leave Importance blank for that candidate need.

You are encouraged to elaborate on any of the needs (see Section III.F). If your needs are not among the candidates, feel free to add them (see Section III.E). See Section IV for a further explanation of some of the candidate IT security needs.

III.A. NEEDS RELATED TO POLICY, MANAGEMENT, AND PLANNING

These statements address the need for clear, unambiguous, unifying/encompassing statements of agency responsibility with respect to the management and protection of information technology resources, what needs to be protected, what IT security management and technical activities are required, when they are to be performed, and who bears what responsibility.

KEY: TYPE OF CANDIDATE IT SECURITY NEED: [A]=assistance, [G]=guidance, [P]=policy, [PR]=products, [S]=standards, [T]=technology, [TI]=technical information. IMPORTANCE: N=none or not applicable, L=low, M=moderate, H=high, V=very high. IMMEDIACY: IM=immediate (within 1 year), NT=near term (1-3 years), LT=long term (more than 3 years). See Section IV for further description of candidate needs.

INFORMATION TECHNOLOGY (IT) SECURITY NEEDS RANKED BY IMPORTANCE AND IMMEDIACY			
Need ID	Candidate IT Security Need	Importance (N,L,M,H)	Immediacy (IM,NT,LT)
Federal Policy:			
A1	[P] integrating all IT security-related federal policies and directives		
A2	[P] on designating an owner for sensitive data, systems, and networks		
A3	[P] promoting IT security policy awareness among executive level functional and technical management		
A4	[P] incorporating "ethics" into Office of Personnel Management (OPM) training regulations		
A5	[P] on IT security as an integral part of the system development life cycle		
A6	[P] related to information collection, dissemination, and sharing		
A7	[P] on establishing an emergency response capability		
Agency IT Security Management and Planning:			

A8	[G] on developing an agency/organization IT security policy		
A9	[G] [S] defining information and system sensitivity and criticality levels		
A10	[G] on computer security planning at the management level		
A11	[G] on developing security plans		

III.B. NEEDS RELATED TO BASIC IT SECURITY FUNCTIONS AND ACTIVITIES

These statements address the need for help with knowing what to do and how to perform such basic IT security functions of: risk analysis, the selection and implementation of cost-effective controls, periodic review and certification, IT security planning, continuity of operations, personnel security, assignment of IT security responsibility, and security awareness and training.

KEY: TYPE OF CANDIDATE IT SECURITY NEED: [G]=guidance, [P]=policy, [PR]=products, [S]=standards, [T]=technology, [TI]=technical information. IMPORTANCE: N=none or not applicable, L=low, M=moderate, H=high, V=very high. IMMEDIACY: IM=immediate (within 1 year), NT=near term (1-3 years), LT=long term (more than 3 years). See Section IV for further description of candidate needs.

INFORMATION TECHNOLOGY (IT) SECURITY NEEDS RANKED BY IMPORTANCE AND IMMEDIACY			
Need ID	Candidate IT Security Need	Importance (N,L,M,H)	Immediacy (IM,NT,LT)
B1	[G], [P], [A] to perform a risk analysis		
B2	[G], [A] to develop contingency and continuity of operations plans		
B3	[G], [T], [A] on quantifying the impact of security violations and breaches		
B4	[G], [A] doing disaster recovery testing		
B5	[G], [A] on establishing an agency emergency response capability		
B6	[G], [A] doing independent security verification reviews of IT security plans and described controls		
B7	[G], [A] doing certifications and accreditations		
B8	[G] [A] developing a comprehensive personnel security program		
B9	[G] [P] [A] and materials for IT security awareness and training		

III.C. TECHNICAL APPROACHES, METHODOLOGIES, PRODUCTS

These statements address the need for help in addressing specific technical concerns, technologies, and environments with a variety of specific technical solutions.

KEY: TYPE OF CANDIDATE IT SECURITY NEED: [G]=guidance, [P]=policy, [PR]=products, [S]=standards, [T]=technology, [TI]=technical information. IMPORTANCE: N=none or not applicable, L=low, M=moderate, H=high, V=very high. IMMEDIACY: IM=immediate (within 1 year), NT=near term (1-3 years), LT=long term (more than 3 years). See Section IV for further description of candidate needs.

INFORMATION TECHNOLOGY (IT) SECURITY NEEDS RATED BY IMPORTANCE AND IMMEDIACY			
Need ID	Candidate IT Security Need	Importance (N,L,M,H)	Immediacy (IM,NT,LT)
Areas of Concern:			
C1	[TN] [PR] for access control and authentication		
C2	[TN] [G] on public access by "client" populations		
C3	[PR] [G] on user accountability		
C4	[G] [S] defining minimum security controls for defined sensitivity levels		
C5	[PR] [S] satisfying national/international criteria		
C6	[TL] [PR] [TN] [G] for "troubleshooting" IT security problems		
C7	[P] [G] on electronic data interchange, public key encryption, digital signatures, and electronic authentication		
C8	[TL] [PR] for incorporating IT security in software development and software engineering		

C9	[TI] on computer security tools (evaluations)		
Specific IT Security Environments:			
C10	Minimum security standards for LANs and [TL] [PR] [G] to manage and protect LANs		
C11	[G] [PR] [TPI] on linking PCs to LANs to mainframes in one security architecture		
C12	[G] on integrating open system environment products		
C13	[G] [TN] for secure dial-in and the use of laptops		
C14	[G] on database security		

III.D. NEEDS RELATED TO ACCESS TO AND THE SHARING OF IT SECURITY INFORMATION

These statements address the need for conveniently and efficiently obtaining access to and sharing of timely, relevant IT security information produced by a variety of central agencies, other agencies, and other organizations.

KEY: TYPE OF CANDIDATE IT SECURITY NEED: [G]=guidance, [P]=policy, [PR]=products, [S]=standards, [T]=technology, [TI]=technical information. IMPORTANCE: N=none or not applicable, L=low, M=moderate, H=high, V=very high. IMMEDIACY: IM=immediate (within 1 year), NT=near term (1-3 years), LT=long term (more than 3 years). See Section IV for further description of candidate needs.

INFORMATION TECHNOLOGY (IT) SECURITY NEEDS RATED BY IMPORTANCE AND IMMEDIACY			
Need ID	Candidate IT Security Need	Importance (N,L,M,H)	Immediacy (IM,NT,LT)
D1	Clearinghouse of IT security information		
D2	Better flow of information from NIST to users		

III.E. OTHER IT SECURITY NEEDS

Use this section to identify additional IT security needs and to specify priorities for them.

KEY: TYPE OF CANDIDATE IT SECURITY NEED: [G]=guidance, [P]=policy, [PR]=products, [S]=standards, [T]=technology, [TI]=technical information. IMPORTANCE: N=none or not applicable, L=low, M=moderate, H=high, V=very high. IMMEDIACY: IM=immediate (within 1 year), NT=near term (1-3 years), LT=long term (more than 3 years). See Section IV for further description of candidate needs.

INFORMATION TECHNOLOGY (IT) SECURITY NEEDS RATED BY IMPORTANCE AND IMMEDIACY			
Need ID	Candidate IT Security Need	Importance (N,L,M,H)	Immediacy (IM,NT,LT)
E1			
E2			
E3			
E4			
E5			

III.F. FURTHER DESCRIPTION OF DESIGNATED NEEDS AND ADDITIONAL COMMENTS

Use this space to provide additional comments and to further elaborate on selected IT security needs. Please specify which IT security needs are being referenced.

SECTION IV
FURTHER DESCRIPTION OF CANDIDATE IT SECURITY NEEDS

The following are further descriptions of the candidate IT security needs used in Section III, above.

SECTION A - NEEDS RELATED TO POLICY, MANAGEMENT, AND PLANNING

These statements address the need for clear, unambiguous, unifying/encompassing statements of agency responsibility with respect to the management and protection of information technology resources, what needs to be protected, what IT security management and technical activities are required, when they are to be performed, and who bears what responsibility.

NEED ID	IT Security Need
Federal Policy:	
A1	Policy and guidance on integrating all IT security-related federal policies and directives, covering computer security, internal controls, financial management controls, information resources management (IRM), acquisition, and personnel
A2	Policy requiring the designation of an owner for sensitive data, systems, and networks relating such designation to the responsibility for the security of the data, systems, and network components; such policy would help define system boundaries and require coordination by the data/system/network owner with organization IRM and IT security management to assure required levels of protection
A3	Policy, guidance, and training promoting IT security policy awareness among executive level functional and technical management
A4	Policy on incorporation of "ethics" into Office of Personnel Management (OPT) training regulations

A5 Policy defining IT security as an integral part of the system development life cycle

A6 Policy related to collection and dissemination of information and information sharing (among federal, state, private sector, and other organizations) covering privacy, computer matching, and trans-border data flow

A7 Policy on establishing an emergency response capability

Agency IT Security Management and Planning:

A8 Guidance on developing an agency/organization IT security policy

A9 Guidance and standards defining information and system sensitivity and criticality levels

A10 Guidance on computer security planning at the management level, including guidance on the placement of IT security activities/functions in the organization so as to avoid security fragmentation

A11 Guidance on how to develop IT security plans

SECTION B - NEEDS RELATED TO BASIC IT SECURITY FUNCTIONS AND ACTIVITIES

These statements address the need for help with knowing what to do and how to perform such basic IT security functions of: risk analysis, the selection and implementation of cost-effective controls, periodic review and certification, IT security planning, continuity of operations, personnel security, assignment of IT security responsibility, and security awareness and training.

NEED ID Need	IT Security
B1	Guidance, products, and assistance to users on performing a risk analysis of their systems, including useful/practical samples or models
B2	Guidance and assistance to users to develop contingency and continuity of operations plans for their systems, including useful/practical samples or models
B3	Guidance, tools, techniques, and assistance on quantifying the impact on confidentiality, integrity, and availability of security violations and breaches
B4	Guidance and assistance in doing disaster recovery testing
B5	Guidance and assistance on establishing an agency emergency response capability
B6	Guidance and assistance in doing independent security verification reviews of plans prepared in accordance with directives (currently OMB Bulletin 90-08) and identifying whether the controls reported in these plans are correctly implemented
B7	Guidance and assistance in doing certifications and accreditations, including certifying Commercial-Off-the-Shelf (COTS) software and systems
B8	Guidance and assistance in developing a comprehensive personnel security program, including personnel security, personnel screening, assignment of IT security responsibility, and security awareness and training
B9	Guidance, assistance, course outlines, lessons plans, handouts, training aids, and other instructional materials for IT security awareness and training

SECTION C - TECHNICAL APPROACHES, METHODOLOGIES, PRODUCTS

These statements address the need for help in addressing specific technical concerns, technologies, and environments with a variety of specific technical solutions.

NEED ID	IT Security Need
Areas of Concern:	
C1	Technical approaches (such as products and methodologies) for controlling access to agency/organization IT resources and for authenticating (i.e., verifying the identity of a person and the privilege of that person to do something) federal users and contractor personnel; such advanced technical approaches would replace the sole use of passwords and might employ easy to use, non-threatening physical and behavioral characteristics and passive or smart "tokens"
C2	Technical approaches to and guidance on public access by "client" populations to agency information resources
C3	Products and guidance on achieving user accountability (i.e., that each person is responsible for his/her use of IT resources and all of his/her use can be traced back to him/her)
C4	Guidance and standards defining minimum security controls for defined sensitivity levels
C5	Products and systems satisfying national/international criteria for protection of data and systems and that address integrity and availability in addition to confidentiality
C6	Tools, products, techniques, and guidance for "troubleshooting" (i.e., identifying and resolving) IT security problems; these might include artificial intelligence techniques, decision trees, manual or automated troubleshooting manuals, virus checkers and vaccines, and means of analyzing audit trail logs

C7 Products and guidance on the application of electronic data interchange, public key encryption, digital signatures, and electronic authentication

C8 Tools and products for software development and software engineering that vigorously incorporate IT security
C9 Product evaluations of computer security tools

Specific IT Security Environments:

C10 Minimum security standards for LANs and tools, products, and guidance to manage and protect LANs

C11 Guidance, products, and technical product information on linking PCs to LANs to mainframes in one security architecture

C12 Guidance on integrating open system environment products so as to achieve interoperability among the security features of these products

C13 Guidance and technical solutions for low cost, secure dial-in and the use of laptops

C14 Guidance on IT security issues in the use of databases

SECTION D - NEEDS RELATED TO ACCESS TO AND THE SHARING OF IT SECURITY INFORMATION

These statements address the need for conveniently and efficiently obtaining access to and sharing of timely, relevant IT security information produced by a variety of central agencies, other agencies, and other organizations.

NEED ID	IT Security Need
D1	Clearinghouse of computer security information with references to documents by other organizations and agencies - leading to sharing and minimizing duplication of effort, cost, resources, cost.
D2	Better flow of information from NIST on the status of its products, services, and activities, perhaps through a newsletter or other electronic and non-electronic means

APPENDIX C
SELECTED FEDERAL SECURITY-RELATED DIRECTIVES

The following is an extract of Appendix A of NISTIR 4749, Statements of Work for Federal Computer Security Services: For Use In-House or Contracting Out. See that document for a fuller descriptions of applicable laws and directives.

FEDERAL MANAGERS' FINANCIAL INTEGRITY ACT OF 1982 (Pub. L. 97-225)
This law enacted the main provisions of OMB Circular A-123. Its purpose is to ensure that agencies maintain effective systems of accounting and administrative controls against fraud, waste and abuse.

PAPERWORK REAUTHORIZATION ACT OF 1986 (Pub. L. 99-500)
This law clarified the Brooks Act definition of "ADPE" to include telecommunications, ADP services and support services. This law gave permanent protest jurisdiction to the GSA Board of Contract Appeals (GSBCA). Implementation of this law in the Federal Information Resources Management Regulation (FIRMR) resulted in the adoption of the term "Federal Information Processing (FIP) Resources" to encompass all resources defined by the Brooks Act amendment.

COMPUTER SECURITY ACT OF 1987 (Pub. L. 100-235)
This law amends the NBS Organic Act of 1901, Federal Property and Administrative Services Act of 1949 and Brooks Act of 1965 to add provisions on the protection of computer-related assets (e.g., hardware, software, and data). This Act:

- assigns responsibility of development of computer security guidelines and standards to the NIST;
- requires federal agencies identify existing and under development systems that contain sensitive information;
- requires development of a security plan for each identified sensitive computer system; and
- requires mandatory periodic training in computer security awareness and accepted computer security practice of all employees involved with the management, use, or operation of federal computer systems within or under the supervision of a federal agency.

Current instructions for implementing the Computer Security Act are provided in OMB Bulletin 90-08, Guidance for the Preparation of the Security Plans for Federal

Computer Systems that Contain Sensitive Information.

PRIVACY ACT OF 1974 (Pub. L. 93-579)
This law was enacted to provide for the protection of information related to individuals maintained in federal information systems, and to grant access to such information by the individual. The law establishes criteria for maintaining the confidentiality of sensitive data and guidelines for determining which data are covered.

OMB Circular A-130 implements provisions of this act. FIPS PUB 41 provides computer security guidelines for implementing the act.

FREEDOM OF INFORMATION ACT (Pub. L. 90-23)
This law makes federal information readily available to the public. It also establishes the conditions under which information may be withheld form the public to ensure that certain information such as trade secrets be protected.

OMB CIRCULAR A-123, INTERNAL CONTROL SYSTEMS
OMB Circular-123 has specific policies and standards for federal agencies for establishing and maintaining internal controls in their programs and administration activities. This includes requirements for vulnerability assessments and internal control reviews. The main provisions of A-123 became law through the enactment of the Federal Manager's Financial Integrity Act of 1982.

OMB CIRCULAR A-127, FINANCIAL MANAGEMENT SYSTEMS
OMB Circular A-127 has specific policies and standards for federal agencies for establishing and maintaining internal controls in financial management systems. This includes requirements for annual reviews of agency financial systems which build on reviews required by OMB Circular A-123.

OMB CIRCULAR A-130, MANAGEMENT OF FEDERAL INFORMATION RESOURCES
OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, has specific requirements for establishing the agency computer security program. The program should include application security, personnel security, information technology installation security, and security awareness and training programs. It also assigns responsibilities to the Department of Commerce, Department of Defense, General Services Administration, and Office of Personnel Management. Federal agencies are required to address security in their annual

internal control report required under OMB Circular A-123.

APPENDIX D
DISCUSSION OF THE OMB, NIST, NSA AGENCY ASSISTANCE VISITS

In July of 1990, OMB issued OMB BULLETIN 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information. Its purpose was to provide federal agencies guidance on computer security planning activities required under the Computer Security Act of 1987. The Bulletin indicated that visits by OMB, NIST, and NSA staff would be scheduled with agencies to discuss the agency's implementation of the Act. NIST and NSA were to provide technical advice and assistance on the agency's security needs as requested. These visits were completed in the Summer of 1992. A report of that activity has been prepared. The report is entitled, "Observations of Agency Computer Security Practices and Implementation of OMB Bulletin No. 90-08: 'Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information,' February 1993." The following is extracted from the Executive Summary of that report.

Based on the observations of the agency visit team, "OMB, NIST and NSA propose the following steps to improve Federal computer security.

1. Focus Management Attention on Computer Security:
   - OMB will state in forthcoming guidance that lack of compliance with certain computer security requirements should be considered a material weakness under the Federal Manager's Financial Integrity Act.
   - The OMB/NIST/NSA team will again visit agencies that have reported computer security as a "high-risk area."

2. Improve Planning for Security:
   - OMB will require planning for computer security as a critical element of agency IRM planning in its revision of OMB Circular No. A-130, "Management of Federal Information Resources."

3. Update Security Awareness Training
   - NIST, with OPM assistance, will review the computer security awareness and training guidelines to assure they are still viable. Agencies will incorporate these guidelines into their awareness and training programs.

- OMB will revise OMB Circular No. A-130 to require agencies to:
  - Assure that new employees and contractors complete awareness and training before they begin using Federal systems.
  - Assure completion of awareness and training by employees of other agencies before allowing them to access sensitive systems.
  - Assure periodic refresher training for employees and contractors.

4. Improve Contingency Planning and Incident Response Capabilities:
   - OMB will require agencies to:
     - Periodically test contingency plans for their most sensitive systems.
     - Establish formal incident response capability.

5. Improve Communication of Useful Security Techniques:
   - NIST will enhance its efforts to raise awareness of know solutions to security problems.

6. Assess Security Vulnerabilities in Emerging Information Technologies:
   - NIST and NSA will assess the security vulnerabilities inherent in emerging information technologies and provide guidance to help agencies mitigate against those vulnerabilities."

APPENDIX E
STUDY WORKING GROUP MEETING PARTICIPANTS

A study working group, consisting of approximately 30 invited federal and private sector representatives, provided direction to the study. The group met in February 1992 to comment on the overall approach and methodology and again in September 1992 to review the study results. The following are the participants in the September 1992 meeting.

PARTICIPANTS IN THE FEBRUARY 1992 INITIAL PLANNING MEETING

Non-NIST Participants

Mr. Ed Borodkin, NCSC
Mr. Fred Brandt, Department of State
Mr. Richard W. Carr, NASA
Ms. Mary Casey, Department of Justice
Mr. Rob Cowart, Lockheed Space Operations Corp.
Mr. Dan Gambel, Grumman Data Systems
Mr. Dain Gary, Software Engineering Institute
Mr. Frank Guglielmo, Department of Justice
Mr. John Ippolito, Comsis
Ms. Ann Horth, General Services Administration
Mr. Howard Keough, ASIS, Consultant
Mr. Vic Maconachy, National Computer Security Educators, c/o NSA
Mr. Wayne Madsen, Computer Sciences Corp.
Mr. Vic Marshall, Booz-Allen and Hamilton
Ms. Sally Meglathery, ISSA, c/o New York Stock Exchange
Mr. Nick Pantiuk, Grumman Data Systems
Ms. Sadie Pitcher, Department of Commerce
Mr. Steve Smith, Department of Transportation
Ms. Mary Sue Stone, Department of State
Mr. John Tressler, Department of Education
Ms. Diane Vigue, Department of Transportation

NIST Participants

Mr. Jon Arneson; Ms. Patty Edfors; Mr. David Ferraiolo; Mr. Dennis Gilbert; Ms.Irene Gilbert; Ms. Barbara Guttman; Mr. Jerry Linn; Mr. Dennis Steinauer; and Ms. Marianne Swanson

PARTICIPANTS IN THE SEPTEMBER 1992 STUDY RESULTS REVIEW WORKSHOP

NIST and Non-NIST Participants

Ms. Judy Bloom, U.S. Department of Justice
Mr. Ed Borodkin, National Computer Security Center
Mr. Richard W. Carr, National Aeronautics Space Administration
Ms. Dorothea de Zafra, Department of Health & Human Services, Public Health Service
Mr. Donald Franklin, Department of Veterans Affairs
Mr. Bill Garvin, Social Security Administration
Mr. Dennis Gilbert, NIST/CSL
Ms. Irene Gilbert Perry, NIST/CSL
Mr. Stephen W. Greenfield, Department of Health and Human Services
Mr. John Haines, Department of the Interior
Mr. John Ippolito, Comsis
Ms. Rhonda Joseph, Department of Transportation
Mr. William G. Logan, Department of Health and Human Services
Mr. Vic Maconochy, National Computer Security Educators
Mr. Nick Pantiuk, Grumman Data Systems
Ms. Sadie Pitcher, Department of Commerce
Mr. Dennis Steinauer, NIST/CSL
Mr. John Tressler, Department of Education

APPENDIX F

SOURCES OF INFORMATION ON IT SECURITY REQUIREMENTS AND NEEDS

The following documents were identifed by participants at the February 1992 meeting of the study working group as being potential sources of informaiton regarding IT security requirements and needs.

Potential Sources of Information

- NIST Annual Report
- NIST PUBS LIST 91
- Descriptions of related activities by NIST and other organizations
- NIST Framework Handbook outline and description
- OMB Bulletin 90-08, OMB Circular A-130, Notes on A-130 from Computer Security Managers' Forum work group
- PCIE/PCMI Model Framework
- NIST draft - Minimum Security Functionality Requirements (MSFR) for Multi-User Operating Systems (Now NISTIR 5153 "Minimum Security Requirements for Multi-user Operating Systems, A Protection Profile for the U.S. Information Security Standard.")
- NISTIR 4976, Assessing Federal and Commercial Information Security Needs
- NISTIR 4846, Computer Security Course Compendium plus supplement
- Computers At Risk, National Science Foundation
- National Security Agency's "Rainbow Series"
- Security-related publications and directives from GSA, OPM, and GAO
- Reference appendices in NISTIR 4749, Sample Statements of Work for Federal Computer Security Services: For Use In-house or Contracting Out

APPENDIX H
POTENTIAL CANDIDATES FOR ON-GOING CHANNELS OF COMMUNICATIONS

The following was prepared from notes taken by Marianne Swanson, NIST, at a meeting of the channels of communications subgroup, at the February 1992 meeting of the study working group. The session chair for the meeting was Sally Meglathery, ISSA/NY Stock Exchange.

Participants

Mr. Rob Cowart, Lockheed Space Operations Corp.
Ms. Sally Meglathery, NY Stock Exchange/ISSA
Mr. Steve Smith, Department of Transportation
Mr. John Tressler, Department of Education
Mr. Rick Carr, National Aeronautics and Space Administration
Ms. Marianne Swanson, NIST
Mr. Dennis Steinauer, NIST

Need for Open Channels

The channels of communications subgroup began discussion by describing to whom the communications channels should be open. It was agreed that communications with and between NIST and NSA must be kept open at all times. The agencies should be able to communicate not only with NIST and NSA, but also with each other. The idea of an automated network (e.g., Internet) where information is passed back and forth to agencies then down through internal agency e-mail was discussed as a means for rapid transmission of information.

Use of Existing Tools, Mechanisms, and Resources

The idea of an automated network was taken a step further by an example given by one agency. In the example, at an executive working group meeting, twelve executives used specialized software which took their individual ideas, then synthesized the ideas for feedback. The result was a consensus building mechanism that took three to four hours instead of three to four days. This same type of mechanism could be used by NIST to obtain information, agreement, or feedback from various federal agencies on any of a number of IT security-related

issues.

It was agreed by the subgroup that e-mail has many benefits, but the reality is that not all agencies are "connected" to an outside, or even internal, network. The NIST Computer Security Bulletin Board System was discussed as an existing means of disseminating information to any individual who has access to a modem and a personal computer. It was suggested that an index of the bulletin boards' contents be provided routinely. The index should be functional and sorted by topic area and keyword.

An additional use for the bulletin board was brought up. The board could be used to conduct surveys. The bulletin board software has the capability to require or make available to users customized questionnaires.

Another idea for distributing information is for NIST to attach to each new publication a diskette that contains a copy of the publication in (ASCII). This copy can than be posted into agencies' internal e-mail systems.

The discussion on using existing mechanisms concluded with the concept of using the Federal Computer Security Mangers Forum as a vehicle to obtain the needs of agencies. This could be accomplished in a formal manner by placing this "requirement" in the Forum charter. A working group, either within or outside the Forum, could develop the list, then the Forum would validate the list.

Tapping Into Existing Organizations

The subgroup identified a number of existing organizations and recommended that NIST should contact the boards of private and federal groups to get on their mailing lists and to let them know NIST would like to participate in their organizations. By NIST participating at this level, the vendors and groups may "buy into" the standards and policies that NIST is involved with. NIST should make documents available for distribution at the various conferences and participate in the conferences by speaking and vending (i.e., having booths describing NIST products and services). Communications between groups should be two ways -- NIST receiving agency needs and other information, as well as informing the groups what NIST is doing or considering doing.

The subgroup came up with the following list of organizations that could be

targeted by NIST:

- American Bankers Association (ABA)
- American Society for Industrial Security (ASIS)
- Computer Security Institute (CSI)
- Federal Computer Crime Investigators (FCCI)
- Federal IRM Policy Council (FIRMPOC)
- Federal Computer Security Managers' Forum (FCSMF)
- Forum of Incident Response and Security Teams (FIRST)
- Information Systems Security Administration (ISSA)
- Information Systems Security Foundation (ISSF)
- Securities Industries Association

A final way for NIST to become involved is to host a workshop at the National Computer Security Conference where a large working group could validate the list of needs that had been compiled by the Federal Managers Computer Security Forum. The subgroup concluded by agreeing that NIST needs good and continuing feedback at all times.

APPENDIX H
NIST INFORMATION TECHNOLOGY (IT) SECURITY ACTIVITIES

The following is extracted from a NIST brochure describing some of NIST's IT security activities. See the actual brochure for a fuller description of activities. Some of the activities described here are also described in other appendices. Call (301) 975-2934 for additional information. Also see Appendix I for additional related information.

Cooperative Activities with Other Organizations

CSL works closely with users in other organizations to learn about their experiences and needs for technical products and services. By sponsoring and participating in conferences, workshops, and meetings, CSL is able to share information, inform users and vendors of its activities, and learn what others are doing. In addition, CSL responds to requests for advice and consultation, providing direct technical assistance to federal agencies on a cost-reimbursable basis for a limited number of projects related to its program. CSL evaluates computer security methods such as those developed by the National Security Agency (NSA) for the protection of national security information. If investigation shows that these methods can be adapted for the protection of unclassified information, CSL transfers the appropriate technology to other government organizations and to the private sector.

Integrated OSI, ISDN, and Security Program

CSL established a cooperative program to bring together the resources of federal agencies and private organizations to fund specific projects lasting no more than two years each. Tasks covered under this program include the following subject areas: Open Systems Interconnection (OSI); Integrated Services Digital Network (ISDN); network security; computer security; computer-related telecommunications initiatives; network management; data handling; distributed processing; and the interoperability, portability, and scalability of systems. (See Appendix I for additional information.)

Development of Standards

Through participation in national and international standards organizations, CSL contributes to the development of worldwide consensus standards for computers and related telecommunications. Representing the interests of federal

government computer users in industry standards-writing committees, CSL develops standards to meet federal government requirements. When there are no appropriate voluntary industry standards that meet federal needs, CSL may develop the needed standards, frequently with participation by other federal agencies and industry organizations. This has been the case for many of the computer security standards and guidelines.

Research and Outreach

CSL supports the development of conformance test methods that are needed by both vendors and users. Such tests for conformance of products to standards enable vendors to properly implement standards in their computer products. The tests help users determine that the products they acquire are in conformance with standards and are compatible with each other. Test methods and related activities are laboratory-based and frequently conducted cooperatively with other organizations. CSL publishes research findings in reports and technical papers that are disseminated through seminars, workshops, conferences, and user forums.

Solutions to Security Problems

As systems and users become more sophisticated, new and more sophisticated controls will be needed to protect computer information. However, many basic controls are available now and include a broad range of management and technical measures. CSL has developed many of the needed basic controls which have been issued in standards and guidelines covering both management and technical approaches to computer security.

Emergency Response Activities

Recent incidents involving self-replicating computer viruses in computer systems and networks used and operated by the federal government have underscored the need for improved governmentwide coordination and support. For the past several years, CSL has worked closely with other federal agencies to establish emergency response capabilities and to coordinate identification and response to acute computer and telecommunications security incidents.

Risk Management

Implementation of effective information security measures must be based on a balance between the cost of controls and the need to reduce risk or expected loss. "Absolute" security could be achieved only at unlimited cost. Since federal agencies cannot spend unlimited funds to achieve complete security, CSL is investigating risk management techniques that will help agencies identify risks and select cost-effective control measures. In cooperation with NSA, a risk management laboratory has been established for study of these problems.

Contingency Planning

Since computers and networks fail, often leaving users unable to accomplish critical processing, CSL has developed guidance to assist users and managers in providing effective contingency planning. Effective planning and operational procedures are needed to assure that critical applications and data are available in a timely manner.

Computer Security Framework

A comprehensive framework is being developed to guide federal managers in their efforts to identify, implement, and assess the relative cost and adequacy of security controls in computer and communications environments. The framework will also provide an introduction to the field of information security. (See Appendix I for additional information.)

Technical Solutions

Security technology includes standards and guidelines for network security, data encryption, message authentication, network access controls, and trusted technology. Access control, authentication, integrity, confidentiality, and non-repudiation services will be needed to support an Open System Environment (OSE), a conceptual framework that provides a set of information system building blocks with associated interfaces, services, protocols, and data formats. The integration of different systems, architectures, and networks raises computer security concerns and the need to address security in a unified way. CSL is working with the voluntary standards community to develop an OSE security architecture that identifies network security services, the placement of those services within the network, and mechanisms to implement the services. CSL also

works with the Open System Environment Implementors Workshop (OIW) to identify needed security standards.

Future Activities

As technology changes and the use of computer and communications technology increases, there will be greater demand by both government and industry for additional tools to protect sensitive information, especially in open, distributed systems.

Formal Methods. The interconnection of complex systems for "off-the-shelf" components will increase the need for formal methods to determine security requirements and capabilities.

Network Design. High-speed data networks for connecting high-speed computers will need security solutions that are part of the network design, not afterthoughts.

Integrated Security Controls. Techniques will be needed for integrating security controls throughout the life cycle of systems.

Threat Prevention and Detection. Security awareness will continue to be a high priority. As networks are interconnected, there will be increased requirements to prevent and detect potential threats to these systems.

Publications

The NIST Special Publication 500 series, Computer Systems Technology; the NIST Special Publication 800 series, Computer Security Technology; and NIST Interagency Reports (NISTIRs) are available for sale by the Government Printing Office (GPO) or the National Technical Information Service (NTIS). Security awareness guides for users, managers, and executives have been published to assist federal employees in improving computer security practices. Call CSL Publications at (301) 975-2821 for a copy of NIST Publication List 91, Computer Security Publications. In addition, CSL publishes a quarterly newsletter which often features articles on computer security and FIPS activities relating to systems security issues. New publications and upcoming technical conferences are also covered.

Managers' Forum

The Federal Computer Security Managers' Forum is an ongoing opportunity for

federal managers to share information, build upon the experience of other agencies, and avoid duplication of effort. The forum promotes broad dissemination of useful computer security materials within the federal government in a timely manner.

Computer Security Planning

Office of Management and Budget, NSA, and CSL staff members have visited federal agencies to discuss their computer security programs, the implementation of security plans, and the security of systems. Reinforcing the need for continued management awareness and support for computer security planning, these visits followed a joint NIST/NSA review of agency computer security plans in 1988-89. NISTIR 4409, 1989 Computer Security and Privacy Plans (CSPP) Review Project: A First-Year Federal Response to the Computer Security Act of 1987, describes the review effort in detail.

Training

Computer security training conducted by federal agencies helps to increase staff awareness of the need for computer security. CSL issued NIST Special Publication 500-172, Computer Security Training Guidelines, to assist agency personnel to implement the computer security training requirements of the legislation. Broad enough to be applicable in all federal agencies, the guidelines are organized by audience categories, training content areas, and knowledge and skill areas to assist agencies in developing or acquiring training programs that meet their specific needs. NISTIR 4846, Computer Security Training & Awareness Course Compendium, assists federal agencies in locating computer security training.

Validation Services

To support the use of the DES by both the federal and private sectors, CSL validates commercial devices for correct implementation of the data encryption, message authentication, and key management standards. This benefits both buyers and sellers of data encryption devices. When purchasing devices validated by CSL, consumers are assured that the devices were designed properly and that they are compatible with other devices that implement the standard. Developers of devices have stable standards that they can incorporate into a variety of products and sell to users in government and the private sector.

APPENDIX I
ADDITIONAL NIST IT SECURITY-RELATED ACTIVITIES

This appendix describes the following NIST IT Security-related activities:

- *NIST Computer Security Interagency Information Sharing Center (CSIISC) (Clearinghouse)*
- *NIST Framework Handbook (Currently Under Development)*
- *NIST Computer Security Bulletin Board System*
- *National Computer Security Conference*
- *Federal Computer Security Program Managers' Forum*
- *Forum of Incident Response and Security Teams (FIRST)*
- *NIST Integrated OSI, ISDN, and Security Program*
- *NIST Study on Assessing Federal and Commercial Information Security Needs*
- *NIST Minimum Security Requirements and Federal Criteria Efforts*

Also see Appendix H.

NIST Computer Security Interagency Information Sharing Center (CSIISC)

The Computer Security Interagency Information Sharing Center (CSIISC), under NIST, is a clearinghouse which maintains a variety of information systems security documentation for the purpose of sharing with other federal agencies. In order to encourage participation, we have proposed that the CSIISC be a joint effort in that users are required to contribute information.

Examples of documentation that are maintained are: computer security policy statements; certification/accreditation procedures; risk assessment methodologies; computer security position descriptions; position papers, and work-in-progress of major computer security efforts underway by federal departments and agencies. Also, the CSIISC maintains pertinent laws, circulars, bulletins and the like with regard to information security. Additionally, the CSIISC has a variety of training materials, including training videos.

The CSIISC is a complementary activity to that of the NIST Computer Security Bulletin Board System. (See Appendix M for a description of the BBS.)

NIST Framework Handbook (draft currently under development)

The following is a brief description of the NIST framework handbook, a draft of which is currently under development. Selected draft chapters of the document are being released in the form of CSL Bulletins, to make the information they present available more rapidly.

The purpose of this handbook is to provide assistance to managers who are trying to secure their resources. This handbook serves as an introduction to the field of security. It highlights security considerations and methods. The handbook will assist managers understand the important concepts, cost considerations, and interrelationships of security controls. This knowledge is vital for managers to make informed decisions about which types of controls are appropriate within their environments. This handbook does not describe detailed steps necessary to implement an security program. Rather, it provides references to how-to books and articles that provide further detailed information.

This handbook targets federal employees who have security responsibilities, but need assistance in understanding IT security concepts and techniques. The handbook will help the reader to gain an understanding of their IT security needs and develop a sound security approach.

While the Handbook is primarily a management guide, it assumes that the reader has a basic familiarity with IT systems. The handbook does not require the reader to have any familiarity with IT security.

The target reader of this handbook has direct responsibility for the protection of Federal information and/or computing resources (federal interest) and the authority to allocate/reallocate resources to implement security controls. The target reader could be a program, project, or system manager or staff member. This could include federal, state, contractor, or grantee employees.

Although the handbook is targeted for federal employees, the concepts presented are equally applicable to the private sector, as are the cost considerations and interdependencies. While there are many differences between federal and private sector computing, especially in terms of priorities and legal constraints, the underlying principles of IT security and the available safeguards are the same.

This Handbook is divided into five sections:

- Section 1 - Overview - The Overview contain three subsections: the Introduction; the Approach to Security; and Threats, Vulnerabilities and Risk. The Approach to Security explains the underlying principles of IT security and serves as a basic introduction. The Threats, Vulnerabilities and Risk provides background to the reader on some key aspects of IT security.
- Sections 2,3,4 - The next three sections, Management, Operational, and Technical Controls, provide the reader with information about specific controls. The categorization of the controls into three areas was done as an aide to the reader in locating information on specific areas or topics. Most of the controls cross the boundaries between management, operational, and technical. Each chapter within the three controls sections will discuss the basic concepts of the control, the cost considerations, and the interdependencies with other controls.
- Section 5 - This section will provide practical examples on how to implement the protections described in the previous sections.

NIST Computer Security Bulletin Board System

The following information is extracted from a NIST brochure describing the computer security bulletin board system.

The National Institute of Standards and Technology's Computer Security Division maintains an electronic bulletin board system (BBS) focusing on information systems security issues. The security bulletin board is operated as part of the NIST Computer Security Resource and Response Center. It is intended to encourage sharing of information that will help users and managers better protect their data and systems. The BBS contains the following types of information:

- awareness and reference materials
- bibliographies of security-relevant publications
- lists of security-related seminars and conferences
- recent NIST and other publications that deal with security issues
- software reviews
- archive of computer security incident alert information issued by

various computer security response centers
- information about actual incidents and how to protect against or correct known system vulnerabilities

The bulletin board system contains three subsystems:
- The bulletin subsystem consists of eight topic menus with numerous bulletins listed under each topic. Each bulletin contains a limited amount of information, normally consisting of one to three pages. The bulletins can be viewed on the computer screen or can be downloaded (i.e., transferring the entire file to the user's system) for future reference.
- The file subsystem consists of larger amounts of information that can only be viewed by "downloading." The files are separated into directories that can be viewed prior to selecting files to download.
- The message subsystem permits users and the system operator (sysop) to exchange short messages, primarily for administrative or informational purposes.

The BBS is available 24 hours a day, seven days a week. Each BBS user has a maximum of 70 minutes a day, 60 minutes on one call. With a modem, dial (301) 948-5717 for 300, 1200 or 2400 baud rate or dial (301) 948-5140 for 9600 baud rate. To access the BBS via the Internet, use the telnet command, for example: Type 'telnet csrc.nist.gov' or 'telnet 129.6.54.11'

The BBS is menu driven and offers an on-line help feature. If more assistance is required, an extensive user's guide for operating all major functions of this BBS is available.

For further information, a copy of the BBS brochure, or a copy of the BBS User's Guide contact:

National Institute of Standards and Technology
Computer Security Bulletin Board System (CS/BBS)
A-216 Technology
Gaithersburg, MD 20899
(301) 975-3359

National Computer Security Conference

The National Computer Security Conference is a professional conference sponsored by the National Institute of Standards and Technology's Computer Systems Laboratory (NIST/CSL) and the National Security Agency's National Computer Security Center (NSA/NCSC).

The conference has been held annually for approximately the past 15 years in the Baltimore-Washington area. It typically covers three and one-half days during which representatives from government, industry, and academia share information and learn of new ways to apply information security technology. It offers multiple tracks for the needs of users, vendors, and the research and development communities. The conference is usually attended by 1,500 - 2,000.

For additional information about the conference, contact the NIST/NCSC conference registrar at 301-975-2775.

Federal Computer Security Program Managers' Forum

The following is taken from material prepared by the Federal Computer Security Program Managers' Forum.

As a result of its leadership mandate in the Computer Security Act of 1987, the National Institute of Standards and Technology organized the Federal Computer Security Program Managers' Forum. The Forum provides an ongoing opportunity for managers of federal computer security programs to exchange information of use to other programs, build on the experiences of other programs, and reduce possible duplication of effort. The Forum promotes broad dissemination of useful computer security materials within the federal government in a timely manner. The Forum addresses issues related to the security of unclassified federal computer and telecommunications systems. For further information, call NIST at 301-975-3868.

Forum of Incident Response and Security Teams (FIRST)

The Forum of Incident Response and Security Teams (FIRST) is a group of incident

response teams whose members work together voluntarily to deal with computer security problems and their prevention. The objective of FIRST is to further communication among Computer Security Incident Response Capabilities (CSIRCs) and to foster increased participation in incident response-related activities. There are two types of participation in the forum. Forum Members are incident response teams that assist a defined constituency in preventing and handling computer security-related incidents. Liaisons are individuals or representatives of organizations other than emergency response teams that have a legitimate interest in and value to the forum. Government and private sector organizations in North America and Europe participate. For information call 301-975-3411.

NIST Integrated OSI, ISDN, and Security Program

The following was supplied by the NIST Integrated OSI, ISDN, and Security Program staff.

The National Institute of Standards and Technology has initiated the Integrated OSI, ISDN and Security (IOIS) Program in order to bring together the resources of federal agencies and private organizations to address technology issues associated with all aspects of distributed systems. The IOIS Program is designed to be a multi-organization, multi-year activity with specific projects lasting no more than two years each. A few of the subject areas included in this program are Open Systems Interconnection, Integrated Services Digital Network, network security, distributed processing and telecommunications security. The objectives of the IOIS Program are to provide a coordinated and cooperative program for government and industry; to provide federal agencies with assistance in emerging computer, communications, and/or security issues; and to assure integration of integrity and security into communications and computer technologies.

NIST Study on Assessing Federal and Commercial Information Security Needs

The following is extracted from NISTIR 4976, Assessing Federal and Commercial Information Security Needs. Call (301) 975-2934 for additional information.

Federal government and private industry relies heavily on information processing systems to meet their individual operational, financial, and information technology

requirements. Corruption, unauthorized disclosure, or theft of resources have the potential to disrupt operations and could have financial, legal, human safety, personal privacy, and public confidence impact.

Each organization interviewed exhibited unique security characteristics described in terms of the organization's missions and goals. Security needs were further characterized from system to system within an organization.

System and organizational security requirements were found to be based on a higher set of environmental and policy factors and conditions. Computer security technology is applied uniquely in each situation even though there are common concerns.

Because each organization has unique security needs, security products have been applied on a case by case basis to meet individual security threats and concerns. Products should be flexible enough to serve a broad spectrum of security needs at the operating system level, the application level, the organizational level, and the site level. Organizational security requirements also change over time and cannot be totally specified at the time of product acquisition.

For organizations that process unclassified sensitive information, the availability of a greater variety of trusted products that go beyond C2 in terms of functionality and flexibility is needed. There is a demand to address data integrity in a more direct and user friendly manner. Vendors should consider new mechanisms that directly address discretionary and non-discretionary controls, such as role-based access controls, separation of duties, separation of transactions, and user-oriented least privilege.

Most organizations felt security standards should include a wide range of assurances including a "generally accepted commercial practice" level. This new level should minimize the cost of developing new systems or retro-fitting new security functionality in existing systems.

Nearly all of those interviewed expressed the desire to have an independent third party give a "stamp of approval" with regard to the trustworthiness of the systems they were buying. However, the current evaluation and certification process (i.e., with respect to a TCSEC class) was not perceived by users as meeting their needs

for a variety of reasons.

Those interviewed felt that security standards have failed to emerge allowing comprehensive implementation to integrate security across a multi-vendor environment. A system should provide a single user view of security services across a wide range of operating systems. Security features should inter-operate with other security services on both local and remote machines, without the need to train users in new security products. Security technology must support users working effectively together, sharing information, resources and network applications from whatever desktop device they choose within their authority, while providing a common set of security services.
The findings of this study have attempted to identify basic security needs of IT product users, administrators, developers, and evaluators based on actual organizational practices. Although the findings of this study should not be considered conclusive, it is hoped that they will be contemplated in the development of future protection requirements, standards, guidelines and evaluation programs.

NIST Minimum Security Requirements and Federal Criteria Efforts

The following is extracted from NISTIR 5153 "Minimum Security Requirements for Multi-user Operating Systems, A Protection Profile for the U.S. Information Security Standard." Call (301) 975-2934 for additional information.

The Minimum Security Requirements for Multi-User Operating Systems (MSR) document provides basic commercial computer system security requirements applicable to both government and commercial organizations. These requirements include technical measures that can be incorporated into multi-user, remote-access, resource-sharing, and information-sharing computer systems. The MSR document was written from the prospective of protecting the confidentiality and integrity of an organization's resources and promoting the continual availability of these resources. The MSR presented in this document form the basis for the commercially oriented protection profiles in Volume II of the draft Federal Criteria for Information Technology Security document (known as the Federal Criteria). The Federal Criteria is currently a draft and supersedes this document.

The MSR document has been developed by the MSR Working Group of the

Federal Criteria Project under National Institute of Standards and Technology (NIST) leadership with a high level of private sector participation. Its contents are based on the Trusted Computer System Evaluation Criteria (TCSEC) C2 criteria class, with additions from current computer industry practice and commercial security requirements specifications.

APPENDIX J
ADDITIONAL SOURCES OF IT SECURITY INFORMATION AND HELP

Below are some sources of information for those who are determining security needs or looking for help in addressing those needs. Also see Appendix H and Appendix I.

CSL Bulletins published by NIST

Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Among the bulletins available are those on Data Encryption Standard; Guidance to Federal Agencies on the Use of Trusted Systems Technology; Computer Virus Attacks; Security Issues in the Use of Electronic Data Interchange; The GOSIP Testing Program; FIPS 140 - A Standard in Transition; An Introduction to Secure Telephone Terminals; TCP/IP or OSI? Choosing a Strategy for Open Systems; Advanced Authentication Technology; and Establishing a Computer Security Incident Response Capability. Bulletins are issued on an as-needed basis and are available from CSL Publications, NIST B151, Technology Bldg., Gaithersburg, MD 20899, telephone (301)975-2821 or FTS 879-2821.

Other NIST publications

Call the Computer Systems Laboratory (CSL) at (301)975-2821 to receive NIST Publication List 91, Computer Security Publications, an annotated bibliography of NIST computer security documents. Documents can be purchased through the Government Printing Office (GPO) at (202) 783-3238 and the National Technical Information Service (NTIS) at (703) 487-4780.

The National Computer Security Center (NCSC) Compusec Technical Publications

Known as the "Rainbow Series." Although these documents have been developed to support the processing and protection of classified data, they contain information that may be of value to those with sensitive non-classified environments. Contact (301) 766-8729 for a list of publications.

Glossaries

The NCSC publication NCSC-TG-004, Glossary of Computer Security Terms
CSL has *NISTIR 4659, Glossary of Computer Security Terminology. CSL Bulletin, Bibliography of Computer Security Glossaries,* Sept 1990, describes several glossaries.

NIST Computer Security Bulletin Board System (BBS)
The BBS emphasizes information systems security issues and contains awareness and reference materials, including bibliographies, security-related seminar and conference lists, and information about actual computer security incidents and how to protect against or correct known system vulnerabilities. The BBS number is (301) 948-5717 (300,1200 or 2400 baud); (301) 948-5140 (9600 baud); and voice (301) 975-3359.

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

Risk Management Laboratory
NIST, with NSA, operates a Risk Management Laboratory in Gaithersburg, Maryland which investigates tools and techniques for risk management. Call (301) 975-3359 for more information.

National Computer Security Conference
This large multi-track, multilevel conference, co-sponsored by NIST and NSA, is held annually in the Fall in the Baltimore-Washington area and provides an extensive look at what is happening and what is being sought in security on the part of both the federal and private sectors.

APPENDIX K
DESCRIPTION OF FISSEA AND THE FISSEA DACUM EFFORT

The following description of FISSEA is taken from material prepared by FISSEA.

DESCRIPTION OF THE FEDERAL INFORMATION SYSTEMS SECURITY EDUCATORS' ASSOCIATION (FISSEA)

The purpose of the Federal Information Systems Security Educators' Association (FISSEA) is to:

a. Elevate the general level of security awareness and knowledge within the federal government and federally related workforce.

b. Provide for the exchange of information regarding--and for the improvement of--information systems security training and education programs throughout the federal government, and by its contractors and academic institutions.

c. Provide for the professional development of the members.

The organization, its officers and members, seek to make a difference in information systems security education and training by actively coordinating training developments with educators
involved in program development. Annually, an award is presented to the candidate selected as Educator of the Year honoring distinguished accomplishments in security training.

Membership is open to information systems security professionals, professional trainers and educators, and managers responsible for information systems security training programs in federal agencies - to include the contractors of these agencies and faculty members of accredited educational institutions.

Members are encouraged to participate in the annual FISSEA conference and to serve on any of the standing committees or participate with the ad hoc task groups. Currently, there are four
standing committees involving: conference planning; standards for training courses and materials; resource sharing; and, communications.

An interested individual may become a member upon application to FISSEA, or upon paid registration to attend the annual FISSEA conference. There is no additional membership fee.

Questions and requests for information may be directed to:

PHS/Office of the Asst. Secretary for Health, Ms. Janet C. Jelen, 5600 Fishers Lane, Room 17-53, Rockville, MD 20857, Telephone: (301) 443-6420, Fax: (301) 443-1823

The stated purpose of FISSEA is to safeguard all of the facility, equipment, and data resources used for processing sensitive information. This goal is accomplished through the following
specific objectives:

1. Comparative examination of instructional methodologies with reference to target audience categories;

2. Improvement of training course and materials design, with reference to subject content and intended level of systems security expertise;

3. Improvement of training needs analyses and training evaluation techniques;

4. Cooperative development/sharing of successful methodologies and training materials;

5. Cross-fertilization of ideas and expertise among systems security professionals and professional trainers and educators; and

6. Recognition of individual members' achievements.

MOTTO: A quotation from Christa McAuliffe, the teacher-astronaut who perished in the Challenger disaster in 1986, shall be the organization's motto: "I touch the future; I teach."

Appendix K

DESCRIPTION OF THE FISSEA DACUM EFFORT

The following is a recent effort by the Federal Information Systems Security Educators' (FISSEA) Association. It is described here because the subject matter addressed and the tools employed have potential application to identifying and validating agency security needs determining sources of help in addressing those needs.

Overview

During the week of July 20-24, 1992, FISSEA sponsored a DACUM (develop a curriculum) workshop at a Idaho State University. The workshop brought together a group that had both interest and investment in information technology (IT) security training and awareness. Idaho State University was used because of its group decision support system (GDSS). (Other names for the technology include: electronic consensus building, electronic brainstorming, electronic meeting system, computer-supported cooperative work, and groupware). The facility, called the Simplot Decision Center, (named after a prime sponsor, the Simplot Corp.) was developed, and the workshop was facilitated, by Prof. Corey Schou, chair of the ISU Information Systems Department of the College of Business.

Dr. Schou has been active with the computer security educators. He also led a project that developed, under DoD sponsorship, a set of Information Security Modules suitable for incorporation in courses in colleges of business and information systems programs - the Green Book. He has been evolving his "world class" GDSS at ISU for a while. Corey reports successful workshops with a number of private sector and other organizations.

The version of the software used by the group was developed by the University of Arizona under sponsorship by IBM. IBM has set up a number of GDSSs for their own use and for use of those renting the facilities, using an IBM-developed variation of the UA product. The technology does not mandate that all participants be at the same location.

The workshop was attended by the following:

Mr. Jim Colborn, Indian Health Services
Mr. Duane Fagg, Paragon

Mr. Jim Frost, ISU, Comp. Sci. Faculty,
Simplot Decision Ctr. Operator
Mr. Dennis Gilbert, NIST
Mr. Vic Maconochy, NSA, FISSEA chair, Meeting Host
Ms. Martha Leonette, USPS, ADP Security Branch
Mr. John Mailliard, FBI, Deputy, Regional Processing Center
Ms. Sharon Muzik, Naval Electronic System Enginering Facility
Mr. John Nguyen, USPS, Field Program Training Branc
Ms. Joan Pohly, AF, Cryptologic Support Center
Mr. Jim Powers, Naval Fleet Nemerical Oceanograhpy Center
Mr. Corey Schou, ISU, Meeting Facilitator
Mr. Bill Spano, NSA, National Cryptologic School
Mr. John Tressler, Dept of Education

Workshop Purpose

The purpose of the workshop was to develop "useful" computer security basics training modules based on the "Todd" training framework model presented in NIST SP 500-172 and the new OPM Regulation 5 CFR 930, Training Requirement of the Computer Security Act. It is the intention of FISSEA to take the output from the workshop, clean and complete it, and present the results to NIST as a proposed NIST SP or other appropriate NIST publication. If that is successful, the plan is to do other training categories and present them to NIST for proposed publication.

Success of the Workshop

Dr. Schou speaks of "success" in terms of time to achieve stated objectives, the quality of the product, and the feelings and sense of achievement of the participants. The workshop was highly successful on a number of counts:

- A significant piece of work was accomplished regarding curriculum development for basic security awareness for a range of audience categories. (Note: the five audience categories of SP 500-172 was expanded to eight). (One of the nice things about the approach is that you not only end up with a "product" from the workshop, but the tools capture the various intermediate steps as an audit trail on the process.)

- The workshop demonstrated the potential of electronic brainstorming for curriculum development and for other group decision-making and document development efforts. The group's efforts were significantly advanced by the use of the tools. The process promoted involvement, consensus, and investment in the outcome of the workshop by the participants.

- The workshop provided the audience and ISU with a better understanding of the strengths and limitations of current set of tools and appreciation of those under development. The workshop also pointed out the importance of the facilitator, operator, and group host or sponsor in the process.

- The subject matter and materials identified and developed at the DACUM workshop is a perspective on agency needs regarding security.

Opportunities Offered by the Use of GDSS Technology

The techniques described here have significant potential. Possible areas where these techniques could be cost-effectively used are those in which: a) NIST and other central agencies refine, validate, and keep current their understanding of evolving agency security needs; b) NIST and other central agencies evaluate the effectiveness of directives, products, and services; and c) NIST and other central agencies adjust program priorities to be congruent with constituent needs; d) individual agencies perform similar self-assessments regarding their security programs. e) NIST develops documents in collaboration with committees or other organizations; and f) NIST and other groups participates in other consensus-based activities - e.g., standards development.

Subsequent DACUM Efforts

Based on the success of the July 1992 DACUM (I), DACUMs II and III were held in August 1993 and November 1993, respectively. DACUM I developed awareness briefing material for executives and program and functional managers. DACUM II validated and enhanced the NIST model for relating audience categories, security training areas, and training levels, as presented in SP 500-172. DACUM 3, held in November 1993, significantly refined the common body of knowledge (i.e.,

foundation for security for training, curricula, and testing). Each of the DACUM workshop products has been (or is being) made available to the federal and private sector security communities for their direct use or further refinement.

APPENDIX L
LIST OF TITLES OR JOB RESPONSIBILITIES OF NEEDS STUDY PARTICIPANTS

The following are some of the titles or job responsibilities identified by 87 staff members interviewed in the NIST Federal Agency IT Security Needs Study:

Title or Job Responsibility

- Admin. Officer
- Administration Management of Physical/Logical Security
- ADP Support for Contingency Planning/Disaster
- ADP Program Manager
- Agency AIS Manager
- AIS Support
- All system development and automation
- Any staff-level work including ADP Security
- Application Software Development/Maintenance
- Automation and Security Implementation
- Branch Chief Operations, Program Software
- Budget, Planning, Security, and Personnel
- Cause Development of Software
- Central Audit and Security Requirements
- Chief, Info. System & Equip.
- Comp. Security IRM planning
- Computer Operations
- Computer Security
- Condensed matter research
- Data Center Manager
- Data Management Systems Division IRM
- Data Center Operational Responsibilities
- Data Center Operations Procedures, Tech. Sec
- Director of Security
- Info System Security Programs - Central and National
- Information Security
- IRM Management Program
- LAN, Intelligent Workstation Management Team
- LAN/IRM/Security
- LANS, PCs, Groupware

- Manage ADP Security Program
- Manual Transactions to Application System
- Management of Division
- Management of IRM Scientists
- Managing HQ Computer Security Program
- Network Administrator
- Overall Security
- Oversee Bureau Classification Program
- Overseer Center AIS Responsibility
- PC Computer Maintenance, Network Backup
- Physical Security, Policy, Guidance & Implementation
- Program Office AIS Manager
- Project Manager for Paperless Processing
- Protecting Privacy of Personal Data
- Quality Assurance and Configuration Management
- Security Admin and Operations
- Security (Info. & Physical), Risk Management
- Software Development for Non-Contiguous Trade Stats
- State Disability Determination Services
- Support of Agency AIS Manager
- Supv Computer, Programmer/Analyst, Applications
- System Development and Maintenance
- Systems Programming Security
- Telecom Planning and Policy ADP Security
- Security Coordinator, Software Engineering
- ITSO LAN Administration
- LAB Computer Security
- Security Management
- Security Officer
- NET Security

The following are the titles, occupations, and areas of concern and counts reported by survey respondents. Please note that a respondent could indicate more than one title, occupation, or area of concern.

Title, Occupation, Area of Concern (Count)

Business resumption (3)

Computer security officer (60)
Computer (6)
Configuration mgt (2)
Consultant (1)
Computer/DP operations (31)
Computer/DP vendor(4)
Director (20)
Disaster management (3)
EDP auditor (2)
Functional/line management (19)
Functional/line operations (1)
Industrial security (1)
Information resources management (17)
Law enforcement officer (4)
Network/communications management (4)
Network/communications operations (1)
PC coordinator (6)
Programmer/analyst (14)
Scientist (2)
Systems analyst/programmer (13)

APPENDIX M
DETAILED DISCUSSION OF SPECIFIC FINDINGS AND OBSERVATIONS

This appendix presents detailed material related to the findings and observations made during the agency security needs study. It is intended to complement the discussions in Section IV.C, which were prepared and distilled from material in this appendix. As noted there, each section represents a collection of related thoughts. As may be expected, remarks made in the interviews and additional comments offered by survey respondents do not fall into distinct categories. Overlaps and interrelationships among issues exist. Opinions, comments, and attitudes of study participants are included, in addition to the direct expressions of needs. It is the opinion of the study team that some of these statements made by study participants may be based on an incomplete or inaccurate understanding on the part of the participants, or they may be the result of misinterpretations or miscommunications. They are nonetheless presented here as reported because the study team thinks that wherever "disconnects" exist, they need to be recognized, understood, and addressed. Also note that opinions reported here are not necessarily shared by NIST or the study team members.

As with Section IV.C, the sections here are loosely organized to correspond to the major groupings of groupings of candidate needs as presented in the needs assessment survey. (See Table III-7.) However, there is not a one-to-one mapping of the discussion sections and the survey needs. This is due to the fact that some subjects were raised in the interviews that did not readily lend themselves to a particular candidate need and suggested a different grouping.

The sections below are numbered to correspond to those of Section IV.C. Note that not all sections from Section IV.C are represented in this appendix.

(C.1.a) Concern was Expressed about Dealing with New and Changing Technical and Processing Environments

- Those interviewed said that they wanted to be able to look toward the future - and transition to what is coming. How does an agency change directions? They wanted technical details about future security packages. One interviewee wanted to know what should he put into procurements for systems he is going to get in two years? How much memory should he be buying in PCs to run future security packages? This interviewee wanted a broad *"spectrum*

analysis" of what security packages of the future will do.

- One of the issues faced by some of those interviewed is that some of their workloads are so large, complex, and integrated that some of the off-the-shelf security products can limit performance unacceptably.

- One respondent rated the need for implementation of cost-effective and efficient safeguards in very large, high-volume systems to be *very highly important*. Another, similarly rated the need for products capable of handling new and modern technology and related staff training.

(C.1.d) "Filtering" is Wanted by Users Less Sophisticated about Security Issues and Concerns

- It was clear from the interviews that having voluminous agency policies and procedures was not sufficient to *"get the message across."* Interviewees reported that big packages don't get read. Because of limited time and conflicting demands, they need to know what does or doesn't apply to them. They need synopses. They don't want to read anything *"big"* (unless they know it is the book they need). They need *"direct"* access to the *"right"* information, but they don't have the time to dig for it. Some indicated that the NIST computer security BBS contains useful information, but it is sometimes difficult to find what is needed. They said that a notice on material they receive, such as *"This does / does not apply to you"* would be very helpful in sorting out what they do or don't need. There was also some discussion as to the optimum placement of this *"filtering of material"* support. A number of interviewees felt that, because of limited resources, this could be best implemented at the agency level, rather than at a subunit level.

- Another interviewee saw the need for a way to choose among solution possibilities to security questions and concerns, perhaps using some sort of decision tree.

(C.2) Issues Concerning Security Policy, Management, and Planning

(C.2.a) Many Feel Hampered by Limited Resources and Budgets and

Frustrated in Justifying Security Resources

- In general, those interviewed expressed confidence that their people were capable of performing the necessary security functions, but also voiced concern that there were not enough people to do all of the work.

- Interviewees wanted to know what others are doing in similar situations.

- Some interviewees wanted a separate security budget in order to get appropriate attention and response from management.

- One respondent commented: *"While I personally see the need for an in-depth, standardized security policy and agency enforcement of a policy, the plain and simple fact of today's budgetary restraints allow us to provide a minimum level of involvement in computer security implementation and review. Until such time that congress and the executive branch realize the importance of and critical nature of computer security, I can't see this issue receiving much more than token support and enforcement of existing computer security regulations."*

(C.2.c) Interviewees Want Federal and Agency Security Requirements to be Reasonable and Relevant. They Want Realistic, Practical, Integrated Federal Security Policy, Directives, and Guidance

- Many interviewees expressed a desire to respond to requirements that were reasonable and practical, that contributed to accomplishing their mission, and that reflected an understanding and appreciation of their specific situation and environment.

- In one interview, the group wanted to see a "scaling" of requirements for the security plans depending on the size and type of system. Those interviewed suggested that requirements need also to be "scaled" depending on the sensitivity of information or the sensitivity of the system. This part of the discussion centered around the requirements for plans for PCs and workstations (small systems). The interviewees conveyed an appreciation of the actual or potential sensitivity of those systems.

- One respondent wrote the following: *"Our office's view of this subject is colored by the fact that our systems are very simple, and have local application only.*

Appendix M

We believe the amount of time and attention our office has had to spend on this issue is very far in excess of its payoff for us. We are also concerned for the amount of time spent across the Department (and the paper generated) on security plans. There may be 1,500 or more separate plans produced. I do not for a minute expect that much information can be absorbed or synthesized effectively. I am very concerned that we have created a paperwork Frankenstein."

- One purpose of federal and agency policy and directives is to explicitly define "acceptable" and "unacceptable." Another is to provide a context in which certain behaviors are "expected." Policy needs to also provide an understanding which creates the incentive for the desired behaviors.

- Survey responses showed that candidate needs that directly addressed federal policy ranked just below the top third of the candidate needs.

- The need for a common interpretation of requirements was often repeated by participants.

- There was much confusion and frustration about what is expected of an agency under current policy and guidance.

- One respondent indicated that risk analysis policy needs to be rewritten and that the current use of annual loss expectancy is not realistic. The respondent rated this need *very highly important* and *immediate*.

- Many thought that policy should sustain and encourage good management practices. One group thought that whatever policy changes are made - NO MORE REPORTS! Another felt that security policy should not be pro forma and bureaucratic, and that there should be less policy and more help.

- One group saw the need for OMB leadership in distinguishing "system" versus "management" controls. The group saw the need for consolidated and integrated guidance. Another said that requirements, mandates, etc. should be consolidated into one reference document, because there exists too much overlap in requirements to handle each independently.

- One group expressed a need for general, consistent policy and guidance across networks, PCs, hosts, databases, and specialized services.

- If large differences exist among agencies and environments, how do you determine the level of help to provide? One suggestion was that you give examples based on a "common" configuration, situation, or environment - and then let the user make the necessary situation-specific or environment-specific adjustments.

- Another group identified the need for policy and guidance to help integrate OMB Bulletins A-123 and A-130 and FMFIA reviews. Currently this agency has developed an in-house policy, but they emphasized that OMB needs to take the lead in this area, with NIST providing guidance at the agency level.

- One respondent commented, "In general terms, how can security issues be addressed in coordination with other system assessment requirements? We are interested in eliminating redundant reporting and analysis within" the department.

- Another respondent saw the need for a "Clear separation of DoD security requirements from security" as *very highly important* and *immediate.*

(C.2.d) Security Needs to be Integrated into Overall Management and Planning

- One group felt that system owners, who are the individuals most knowledgeable about the system, should make the security decisions. They felt that this should be done at the lowest level appropriate to the situation.

- Another group acknowledged that their immediate management thinks that security is critical, but they were concerned that their upper-management doesn't recognize that security *"stuff"* (their term) needs to be done. The group said that their upper level managers do not see any value-added results or savings. Given the lack of an apparent payoff, the managers don't want to burden their staffs.

- A number of those interviewed thought that including security in Management by Objective (MBO) performance elements, other performance plans, and position descriptions would be a step in the right direction.

- One respondent suggested the use of case studies to convince management that security has validity and leads to better products. These

studies could show management what happens when both "good" and "bad" security practices are employed. The case studies should be short and provide enough information to keep the manager interested. Another respondent said that policy and standards related to a separate security budget was a *very highly important* and *immediate* need.

- One group thought that management involvement in audits and reviews, with the requirement for senior management sign-off, would be consistent with the spirit of OMB Circular A-130 and lead to more resources in terms of time, people, and dollars. This same group expressed concern about the future interoperability of security services and how that could be accomplished in an environment of increasing interoperability of computer services. This agency needed help in integrating IT, security, and management controls.

(C.2.f) Users are Concerned about Defining, Identifying, and Protecting Sensitive Information and Systems

- One group wanted data categorization/sensitivity rules for sensitive, unclassified information and systems similar to those for protecting classified information and systems.

- One interviewee noted the potential complexity of determining information sensitivity and pointed to the problem related to bringing together or "aggregating" information from different sources. Despite the complexity and the apparent uniqueness of environments and needs, most of those interviewed appeared to be looking for simpler rules regarding what is sensitive and levels of sensitivity. Most agreed that whatever the definitions, they had to be reasonable.

- There appeared to be confusion over the definition of a system, despite some additional guidance in OMB Bulletin 90-08. One group said that would like to see the definition of a system include a "security point of view" with an accompanying discussion of the pros and cons of different security approaches. Concern was also expressed about the appropriate combining of systems for computer security planning and reporting purposes. One group said that they had defined each application of a general purpose system as a system and consequently are doing risk analyses on each of them that are remarkably similar. Other groups noted the issue of PCs in the definition of a system. One group indicated that currently they define each PC as a system and now need 5,000 risk

analyses.

- One group wanted an individual to be assigned responsibility for every information asset. It was unclear how this would be implemented, given that different agencies have different cultures, environments, and needs. One interviewee suggested that such an assignment be as close as possible to those who create the data, saying *"people understand info they create."*

- Another system sensitivity issue concerns data that is non-FOIA releasable. One group reported being required to use protections that they do not think are appropriate for their real threats and real risks. Because of considerations unique to their agency and systems, they often find themselves in situations where the rules regarding protections do not make sense to them.

- Two issues directly related to the definitions of "system" and "sensitive" are: 1) the appropriate controls for each defined system, and 2) certification that a system is adequately protected and on what basis. One interview group wanted to see a "system security features minimal requirements list" for each level of "sensitive system" in each of the general support and major applications system categories.

(C.2.g) Users Want to Know How to Securely Share Information and Resources with Other Agencies and with Industry. A Few also Want Help in Dealing with Vendors and Contractors.

- One group suggested that NIST provide guidance for organizations that share another's facilities. Both user and sponsor should play a role in addressing security needs and concerns.

- Another issue raised was the need to strike a balance between maintaining confidentiality of records versus sharing information cost-effectively within the government and with outside activities (e.g., state). Guidance is also needed by agencies that use another agency's computers to process and provide third-agency access to unclassified data. One group said that they need policy and guidance on responsibility for continuity of service.

- Only 25 percent of the respondents rated developing a personnel security program as *highly important* or *very highly important*. Related issues, however,

were raised in a number of interviews and in remarks by survey respondents. Dealing with vendors was another issue identified by some.

- One group said that it was hard to get industry's attention. This group had a high production volume and other performance concerns that stretched the performance and capacities of their security products to the limits. Help in establishing liaisons with the vendor community and in pooling requirements to motivate vendors to respond to current and projected requirements was a need of this group.

- One group needed guidance to bring contractors and other third parties "up to speed" regarding different security environments.

- Some of the groups indicated that issues dealing with personnel screening, suitability, system sensitivity, clearances, etc., needed to be clarified.

- One of the respondents said that *"one of the best things that could be done to improve overall security is to greatly speed the background investigations required for employee and contractor personnel security clearances."*

- Another respondent desired quick, inexpensive, and realistic personnel screening guidelines.

- Other respondents suggested the following needs with related importance and immediacy values: guidance on equating security training to position type and job responsibilities (4,2); policy and standards for a career series for information systems security professionals (5,1); and assistance, guidance, policy, and standards for writing position descriptions for a computer security officer position (4,1).

(C.2.h) Users Want to Know How to Address Security Throughout the System Development Life Cycle

- One respondent noted that PC or LAN security is generally not considered until after the equipment is purchased and installed; this needs to be addressed at the beginning of the procurement.

- The question of *"What does it mean to do a security plan for a developmental*

system?" was raised by one of the interviewees.

- One respondent noted the need not only for standards and evaluation criteria, but also products that walk the planner and manager through the logical paths (e.g., computer-aided system engineering tools). The respondent said that such product development approaches will ultimately save personnel resources, dollars, and time.

(C.3) Issues Concerning Basic Security Functions and Activities

(C.3.a) The Need for Tools and Guidance Regarding Risk Management Ranked High

- Needs and their related importance and immediacy values included:
  - Methods for scaling the risk analysis process and verifying that controls are in place;
  - Cleaner definitions and equations for risk analysis;
  - Improved software "tools" for risk analysis;
  - Improvements to the risk assessment process, including an improved risk model applied to system development life cycle (SDLC) deliverables and certified government sources for threat, vulnerability, frequency, and safeguard effectiveness (5,1); and
  - Definitive vulnerability assessments (5,1).
  - A standardized methodology for mainframe risk analysis (5,1)

- One interview group noted that even a good risk analysis does not always provide a "good enough" fall back position when something adverse happens. And, the group noted that inevitably it does. There appeared to be a need for better understanding of all aspects of the risk management process.

(3.b) In Protecting Sensitive Systems, Users Want to Know What is Expected, Appropriate, Adequate

- A number of interviewees said they would like to see meaningful checklists. Others said they would like to see something analogous to an Underwriter's Laboratory (UL) seal or NSA's "Orange Book" evaluation process.

- Also reported was the need for a list of items to be used to certify a system. One interviewee said he would like to see a certification process which made use of an automated security assessment tools package for UNIX systems. This package would check a system to see if patches had been installed and that known holes in the operating system had been plugged.

- One respondent said that there is a need for compliance reviews and evaluations to be conducted within each agency. Without such reviews, the respondent noted, the effectiveness of the entire security program within an agency is diminished. There was an implicit request for guidance in that area.

- One interviewee noted that sometimes certification is ignored in situations where systems are shared between and among organizations.

- One interview group cited the need for guidance on software certification.

(C.4) Issues Concerning Security Awareness and Training

(C.4.a) There is Strong Support for Security Awareness and Training

- A number of those interviewed expressed a need for security training. It was noted by some interviewees that NSA unclassified computer security training (which NSA plans to terminate) does not fit their needs. Some felt that a federal security training void exists. They suggested NIST take over this training, or assist in establishing a course. They felt that NIST would be able to include state-of-the-art issues in such a course, and that it would be geared toward their needs. Funding for training did not appear to be an issue, even for those organizations having small security budgets.

- One group recommended that NIST develop and provide training tools that agencies could tailor to their specific needs, for example, a specific training module such as "a good password." The tools should be designed to be flexible for maximum tailoring by the agency and simple so that they can be used by non-computer experts.

- One interviewee noted that the security training that he is required to give his workers is not applicable to his environment. To illustrate the point, the

interviewee gave the example of a requirement of two hours of annual training for a category of staff that made minimal use of computers, when only 1/2 hour of annual training was required in the staff's primary function, which had significant safety and security functions as an integral part. In fact, the interviewee offered that many of these employees weren't sufficiently computer literate to understand two hours of computer security training. The interviewee was unclear as to what organization level (federal, department, agency, bureau) and which SA&T requirements were most contributing to this situation. It was acknowledged that the distinction between "learning objective" and "course content" can be difficult to make.

- A balanced training program, one that is neither too general nor too specific is needed. If requirements are too specific they may ignore the practical realities of individual environments. If they are too general, they run the risk of being bland and meaningless. Achieving the correct mix is difficult to achieve.

- Also needed is a determination of the correct level at which to provide policy, guidance, training, or assistance. One respondent indicated that training program materials and sources should be made available to allow points of contact to tailor offerings. The respondent thought that general training (awareness & agency policies and procedures) needs to be conducted as the agency level.

- One interviewee indicated that the frequency of training should be only as often as necessary. That interviewee said that training should not create a burden. The person was particularly annoyed at the training accreditation burden under the Paperwork Reduction Act, as he understood it to be.

- As with a number of other areas, there was concern about *"reinventing the wheel."* Those interviewed expressed interest in who is doing what in terms of SA&T.

- One interviewee expressed interest in the mechanics and potential benefit of self-education.

- Several people said there is a definite need for security awareness training. One group noted that when auditors visit, their staff are often asked questions they cannot answer. The implication was that these were questions that the staff

should be able to answer. They saw SA&T as part of the remedy. Others, however, thought that auditors needed SA&T. To further underscore a benefit of training, one survey respondent commented that *"I recently participated in a training session for preparing sensitive system security plans. If I had not, many of my responses in that area would have shown higher need for guidance."*

- Another person said that there is a need for agency-specific training. His agency has hired a security professional with an array of talent and experience to assist with the tailoring.

- One group that has heavy contractor involvement, indicated that assuring that contractors are appropriately made aware and trained and "brought up to speed" was a significant concern and burden that was not being easily or fully addressed.

- One group noted the use of a newsletter to get the SA&T information out. Another recommended better feedback to trade journals regarding security issues and concerns.

- A number of those interviewed wanted help in justifying security. One interviewee noted that, for people that he is dealing with, security is an ingrained cultural anchor - and that you just need to convince them computer security is a security issue. Others expressed similar themes in that security was an easier "sell" if users and staff could see it in terms of what is necessary to get their job done, rather than as an additional burden.

- One group noted that when they tried to do continuity of operations and risk analyses, they had to educate themselves. They were not able to find useful material. They happened to "stumble" across some NIST FIPS that helped. They are looking for NIST to provide three types of education/training:
  - Executive-level class on information security
  - Specific education on useful topics
  - Resources to answer questions (e.g., who should accredit systems?)

- One group said that it would like to see "credentials" established for security professionals. The group saw such professionalization as representing potential for raised awareness about IT within the IT community.

- The following are some additional needs related to SA&T as submitted in survey responses with an indication of their (Importance,Immediacy) using the codes described is Section II, above.

Additional Needs (Importance,Immediacy)

- Products capable of handling new and modern technology, and staff training (5,1)
- Guidance on equating security training to position type, job responsibilities (4,2)
- Easy guidelines for IT assessment security needs (4,1)
- More training (5,1)
- Awareness materials - posters, supplies, etc. (5,1)
- Awareness materials - videos, films, pamphlets (5,1)
- Products providing visual information - posters, etc. (3,2)
- Guidance, policy, products, and training in minimum security awareness training guidelines (4,2)
- Training providing training information on security awareness to all federal computer users (4,1)
- Training for management
- PCs - techniques, training awareness
- Awareness training
- Using the latest technology and techniques that provide security

(C.4.b) Executive-level Security Awareness and Training Seen as Necessary to Obtain Management Support

- It was felt that there was a need to help this level of management understand the consequences of implementing or not implementing protections. (NIST SP 500-172 and Appendix K for a description of the FISSEA DACUM effort.)

- One respondent noted that, *"Upper echelons of management need an awareness of the importance of "IT" Security. Managers sometimes have little interest where higher costs are involved. Budgets and staffing in many cases are neglected."*

(C.5) Issues Regarding Technical Approaches, Methodologies, and Products Dealing with Security

(C.5.a) Help is Strongly Needed with Technical Approaches to Satisfy Security Objectives. Help Must Be Simple, Cheap, Practical, and "Real World"

- One respondent wrote, *"It would be extremely useful if NIST clearly defined minimum standards of what is acceptable. Too many of the areas appear to be "gray" and are subject to interpretation. Standards should be clear and should be "real world." Examples and references to current environments; i.e., LANS, WANS, etc., would be useful."*

- One of the groups wanted these characteristics in terms of tools for cheap, reliable access control, including absolute ID, credentialing, and identifying phone callers. They wanted assistance with related technical, administrative, legal, political, and social problems.

- Another group needed a model for risk analysis and contingency planning. They wanted tools for unsophisticated users. Otherwise, they said, there is broad variation, the analysis is too complex, and specially trained people are needed to solve the problem.

- Still another group wanted to simplify both tools and guidance. They find some standards and guidance so complicated there is nothing to do but *"get a contractor and fork over $100K."* In reality, they think they could do a good contingency plan in house, but the standards and guidance don't make it easy to do this. They said that their people *"don't read anything big."*

- The tools should be small and flexible for maximum tailoring by the using agency. The tools should be simple for non-computer experts.

- One group said that they were looking for things that are cheap, fast, efficient, new, innovative, and professional.

(C.5.b) Help is Sorely Needed in Applying Security in LANs, Networks, and Open Systems, and to PCs in These Environments

- One group said that LAN guidance is needed most. New guidance that is being developed must take into consideration that everything is networked. Guidance on what to do and what type of products to use to secure LANs is needed. Currently, most concerns are at the host level, not during transmission.

People need to be aware of the vulnerabilities that are involved in the transmission of data.

- One interviewed group expressed concern because they provide huge amounts of data to other agencies and they are dealing with that amount of data across a network.

- One group was concerned about protection from illegal access over Internet, where there was a great need to provide information and get information, and at the same time protect against the more sophisticated attacks. Interest was expressed in the subject of a secure internet gateway and firewall.

- One of the groups wanted product-specific recommendations and guidance on LANs, including the basic security features for LANs.

- One of the groups interviewed wanted open systems guidance. They want to know where is the *"keeper of the gate"* and how to prevent inappropriate access to information.

- One of the respondents asked for security guideline development for LANs which needs to occur in parallel with LAN and network implementation, not as a de facto standard.

- The following are some of the related needs expressed by respondents or interviewees in this area, with indications of (*Importance,Immediacy*) if appropriate:
    - Policy and guidance for security within a cooperative processing environment. (mainframe to PC; mainframe to LAN) (4,3)
    - Security processing network for distributing large volumes of classified data throughput U.S. and South America (5,1)
    - Guidance, assistance and products for minimum security standards for bridges and routers (5,1)
    - Guidance, standards, assistance, and technical approaches for large wans in developing a plan and performing (5,1)
    - Technical approaches for standard methodology for communications architecture risk analysis (5,1)
    - Guidance and assistance on developing continuity of operation plans for telecommunications activities (4,1)

- Fax security (4,2)
- Protection of Cellular Radio (5,1)
- Guidance, products, and technical approaches on security for electronic dissemination through bulletin boards, anonymous FTP, etc. (4,2)
- Communications & BBS Security Measures (4,1)
- More products and technical approaches for security of PCs, LANS, Unix Systems security products and technical approaches that permit openness and information dissemination, but protect integrity

- It was noted by some of those interviewed that security for mainframes was more mature and many mainframe tools have been developed. More is needed in the area of PCs, LANs, and WANs.

- Some of the PC-related needs expressed by respondents, along with their (Importance,Immediacy) values, were:
  - Access control & authentication need to be extended to PC's (more so than advances ID & authentication) (5,1)
  - Guidance and policy on security requirements for database management systems for micro computers (4,1)
  - Standards and guidance for development of secure microcomputer-based software (4,2)
  - C2 Level of security evaluations of PC security software & hardware (4,1)
  - Minimum security on PCs (4,1)
  - Agency-wide security software for PC's rather than having individual offices do purchasing locally (5,1)
  - Purchasing guidelines for a site license of PC security software (4,1)

(C.5.e) There was Some Interest in Products and Tools to Control Access

- Most seemed to be looking beyond simple passwords and looking for solutions incorporated in products. However, one respondent, who thought ID and authentication should to be extended to PCs, said *"I think proper administration (based on good guidance / procedures) is more important than advanced authentication techniques."*

(C.5.f) There was Moderate Interest in Identification, Authentication, and

Encryption and Some Confusion about Alternatives

- One agency was looking for an electronic signature that could not be questioned by GAO.

- One interviewee wanted guidance on the use of biometrics and an evaluation of biometric products.

- One group wanted guidance and consideration of tradeoffs in the use of personal ID versus terminal ID. This was needed in system design and system development considerations.

- One interviewed group expressed a need for a digital signature program that is cheap (or at least reasonable) to implement, especially with multiple verifications. The group also predicted a problem with non-repudiation for some special category of users who may want to repudiate signatures on receipts.

- Another group wanted assistance with selecting biometrics, smart cards, and tokens.

- One of the concerns raised in a interview session was the need for electronic signatures and electronic documents, but not being able to afford the 20,000 copies of the software package that is required.

- One group was looking for better standards for encryption and approved devices. The person was not clear on what was approved, and by whom.

- One group dealing with much sensitive information wanted to encrypt cheaply, legally, and in a way that would be accepted by auditors.

- Another interviewee spoke of the need for a one-way signature process so that with e-mail you know the source of the message.

- Still another interview group wanted approved Data Encryption Standard (DES) products. Having approved DES equipment is very important to them, and they reported feeling constrained in their security architecture because of not knowing what's approved.

- Some of the additional needs expressed include:
  - EDI, electronic filing, digital signatures in the foreign trade arena.
  - Policy, standards, and technical assistance on the use of electronic signatures as evidence in criminal prosecutions. (5,1)
  - Standards and guidance on public key encryption for distribution of DES keys (5,1)
  - Signatures and authentication of IT data (5,1)

(C.5.g) Federal Criteria, Trusted Products, and the Need for Technical Evaluation of Products Rated Low in the Survey Compared to Other Needs

- Some related needs and comments expressed by the respondents and interviewees include the following:
  - Policy, standards, and technical information on future product evaluations as to which ones will be done by NIST and which ones will be done by the NCSC (4,2)
  - Policy and guidance on NIST approved security products testing/evaluation labs (4,2)
  - Policy, guidance, and standards about new "Federal Criteria" for security
  - Policy and guidance on working with ITCSEC and NIST requirements (5,1)
  - NIST approval should be as common as the "UL" label on electronic appliances so that government procurements meet basic and simple security guidelines.
  - Publishing NIST document that provides trusted system guidance to civilian agencies (replace NSA Orange Book) (4,2)

C.6 Needs and Concerns Related to Security Information and Sources of Help

C.6.b Wanted is a Clearinghouse and the Free Flow of Information about Security

- A number of respondents and interviewees said that they would like to see models or examples of things they needed to do or produce. Agency policies, procedures, computer security programs, training modules, security plans,

contingency and disaster recovery plans were among the things identified.

- One interviewee noted that getting information out is very important and that NIST has authority and structure to do it. So that person's advice was, *"DO IT!"*

- One respondent reported that, *"Faced with increasing budget cuts, agencies are finding it difficult to allocate the administrative and technical personnel resources needed to develop and implement security programs. NIST could function as both the coordinator and provider of standard definitions, technical products, research reports, etc., relating to computer security. Acting as the "electronic" clearinghouse, NIST could coordinate agency efforts and provide a bulletin board service that would effectively, efficiently, and economically implement security mandates. Issues such as "levels" of system sensitivity, computer resource monitoring (in terms of data integrity as well as CPU/memory/I0 applications usage), general support/major application systems "standard" security features (based on, for example, "Orange Book" type criteria) need products developed. If Government agencies have developed some automated and/or manual products, NIST should evaluate and distribute them to other agencies as either models or methodologies."*

- Among the things that respondents and interviewees reported wanting to see as part of the clearinghouse function were the following, with identified (*Importance,Immediacy*):

Additional Needs (Importance,Immediacy)

- Assistance, technical approaches, technical information, and training on centralized collection, categorization & dissemination of product, platform & environment vulnerability, reported incidents, and recommended safeguards (5,1)
- Information on new viruses & education methods (5,1)
- Information on computer security laws pending in Congress (4,2)
- Guidance on security issues and developments concerning IT, from other agencies (4,2)
- Multi agency shared federal radio programs
- Threat history collection (4,1)
- Policy, guidance, and standards related to Bulletin Board Services (5,1)
- Exchange of information between agencies and other organizations to prevent re-inventing the wheel (5,1)

(C.7) Wants and Ideas Regarding the Role of NIST

- Support for an expanded NIST role was voiced. The following is a collection of some of the comments heard by the study team in the interviews relating to NIST:
    - NIST's role and identity are not clearly defined.
    - NIST should be a respected place that they can refer to and gain credence for their position.
    - Agencies look to NIST for answers to some of their security concerns.
    - They want NIST to say "This is OK!"
    - Many wanted advice from NIST, but not simplistic advice.
    - NIST should assess the value of its guidance and the impact of that guidance on agency resources.
    - There is a role for NIST as coordinator of interagency tools.
    - NIST has authority and structure to get information out. It is important that NIST do it.
    - NIST should convince senior management that they should be involved in R&D for security.
    - Need NIST help to justify dollars of security, especially for OMB Circular basics.
    - A NIST role should be to funnel research dollars to areas where it is needed. Perhaps it can do this by working with those agencies actively investigating and developing programs in security, such as DARPA, DOE, NASA, and the USAF.
    - NIST should institutionalize the process of assessing needs. This shouldn't be a one-shot thing.
    - NIST should have a structure and a stronger computer security program. There should be support for the program from a technology, policy, and other perspectives, analogous to what NSA has.
    - NIST should do a better job getting information out.
    - NIST should create theoretical or conceptual models for IT protection. These models would be analogous to the ones that have been developed by DoD and incorporated in the "Orange Book." There is lack of policy in this area.
    - NIST should provide an information service to federal agencies using a model like that provided by private information service companies.

The service would help the user ask the question and solve the problems. The service would provide some answers and refer users to relevant literature. It could incorporate "how to"s and product evaluations. One interviewee said that it is OK with him if NIST did not recommend products as long as NIST describes issues.

- The need to have existing NIST guidance revised and updated is *very highly important* and *immediate*. This is necessary for the guidance to be effective.
- NIST needs an security *"priesthood"* and a structure.
- There seems to be some confusions about the role of NIST documents regarding the degree to which contain direction which is mandatory and which contain only advice and guidance. There is probably misinterpretation on this score.
- Prefer NIST material that isn't *"wishy-washy."*
- NIST should recommend organizational structures by which agencies can implement security programs.
- NIST should distribute videos and other training materials.
- NIST should know where the expertise exists in the community.
- NIST should raise consciousness and increase awareness about threats and vulnerabilities, perhaps by using *"horror stories."*
- NIST should be more proactive, reduce time in getting new or revised standards out and ensure that the user community is informed of these changes.
- Need initiatives and studies from NIST earlier versus later so that timely actions can be taken based on discoveries.

APPENDIX N
DISTRIBUTION OF IMPORTANCE AND IMMEDIACY BASED ON TOTAL RESPONSES

The following table shows the distribution of importance and immediacy values based on total survey responses in terms of total counts and percentages. There were 224 surveys, each with 36 responses to the candidate needs, for a total of 8,064 total responses.

TABLE APX(N)-1
DISTRIBUTION OF IMPORTANCE AND IMMEDIACY RESPONSES

Import-ance	Immediacy				
	No Response	Immediate	Near Term	Long Term	Total
No Response	356 (4.4)	9 (0.1)	2 (0.0)	0 (0.0	367 (4.6)
None or Not Appl.	529 (6.6)	23 (0.3)	25 (0.3)	81 (1.0)	658 (8.1)
Low	192 (2.4)	121 (1.5)	372 (4.6)	893 (11.1)	1,578 (19.6)
Moderate	5 (0.1)	332 (4.1)	1,656 (20.5)	471 (5.8)	2,464 (30.6)
High	5 (0.1)	947 (11.7)	1,111 (13.8)	94 (1.2)	2,157 (26.7)
Very High	25 (0.3)	700 (8.7)	93 (1.2)	22 (0.3)	840 (10.4)
Total	1,112 (13.8)	2,132 (26.4)	3,259 (40.4)	1,561 (19.4)	8,064 (100)

c,ccc - actual count
(pp.p) - percentage of total responses

APPENDIX O
RELATIONSHIP BETWEEN CALCULATED AVERAGE IMPORTANCE AND AVERAGE IMMEDIACY VALUES

The following table shows the relationship between importance and immediacy in survey responses. It indicates that higher levels of importance of candidate needs had associated lower average immediacy values, meaning respondents reported needing them sooner on the average. As noted previously, the average importance value for all responses was 3.12 and the average immediacy value for all responses was 1.93. (See Appendix W for an explanation of the calculation of average importance and average immediacy.)

TABLE APX(O)-1
RELATIONSHIP BETWEEN CALCULATED AVERAGE IMPORTANCE AND AVERAGE IMMEDIACY VALUES

Average Importance	Average Immediacy
1	2.45
2	2.56
3	2.06
4	1.60
5	1.16
3.12	1.93

APPENDIX P
CALCULATION OF AVERAGE IMPORTANCE AND AVERAGE IMMEDIACY VALUES USED IN THE ANALYSIS

In order to rank and further analyze the candidate needs, letter designations used by respondents to report importance and immediacy of each candidate need were converted to numbers. For importance, 0 corresponds to no response, 1 corresponded to *no importance*, 2 to *low importance*, 3 to *moderate importance*, 4 to *high importance*, and 5 to *very high importance*. For immediacy, o corresponds to no response, 1 corresponded to an *immediate need*, a 2 to a *near-term need*, and a 3 to a *long-term need*. Based on these numbers, a "weighted" average importance value and a "weighted" average immediacy value was calculated for each of the 36 candidate needs as follows:

Average *Importance* Value =

$$\frac{IMP(1) + 2*IMP(2)* + 3*IMP(3) + 4*IMP(4) + 5*IMP(5)}{IMP(1)+IMP(2)+IMP(3)+IMP(4)+IMP(5)}$$

where:

IMP(x) = count of survey responses with Importance value x

Average *Immediacy* =

$$\frac{IMM(1) + 2*IMM(2)* + 3*IMM(3)}{IMM(1)+IMM(2)+IMM(3)}$$

where:

IMM(x) = count of survey responses with Immediacy value x

The overall weighted average Importance ranking for all candidate needs is 3.12. An importance value of 3.00 would equate to a rating of *moderate importance*. The overall weighted average Immediacy ranking for all candidate needs is 1.93. An immediacy value of 2.00 would equate to a rating of *near term immediacy*.

APPENDIX Q
RANKING OF IMPORTANCE OF CANDIDATE NEEDS AMONG ALL RESPONDENTS AND SELECTED GOVERNMENT GRADES

KEY TO TYPE OF CANDIDATE SECURITY NEED: A=assistance; G=guidance; P=policy; PR=products; S=standards; TA=technical approaches; TI=technical information

TABLE APX(Q)-1
RANKING OF IMPORTANCE OF CANDIDATE NEEDS AMONG ALL RESPONDENTS AND SELECTED GOVERNMENT GRADES

Need No.	Candidate Need	All	13/14	15/SES
C10	S/G/TA/PR-LANs	1	1	2
C11	G/PR/TI-linking PCs/LANs/MFs in 1 ITS architecture	2	2	1
C14	G-database security	3	4	4
A05	P-ITS in system development life cycle	4	5	8
B02	G/A-contingency and disaster recovery plans	5	6	8
C13	G/TA-secure dial-in and laptops	6	9	5
A03	P/G/TR-executive/mgt SA&T	7	10	9
A09	**G/S-defining sensitive systems**	8	8	19
A10	**G-developing security plans**	9	3	22
B01	G/PR/A-risk analysis	10	7	15
C12	**G-integrating open system products**	11	26	6
A06	P-collection, dissemination, sharing	12	12	7
A01	P/G-integrating ITS policies and directives	13	20	16
B09	G/PR/A/materials-Security Awareness and Training	14	11	11
D01	**Clearinghouse of ITS information**	15	15	25
A07	P-emergency response capability	16	22	14

Appendix Q

TABLE APX(Q)-1
RANKING OF IMPORTANCE OF CANDIDATE NEEDS AMONG ALL RESPONDENTS AND SELECTED GOVERNMENT GRADES

Need No.	Candidate Need	All	13/14	15/SES
C07	G/PR-EDI, PKE, DS, and elec. authentication	17	19	12
A02	P-owner of sensitive systems	18	14	10
A11	**G-management-level ITS planning**	19	16	30
B03	G/TA/A-impact of security violations	20	21	18
C08	TA/PR-ITS in s/w development and s/w engineering	21	19	13
C04	G/S-minimum controls for sensitivity levels	22	13	17
C09	TI-computer security tools (evaluations)	23	27	24
D02	Better flow of info from NIST to constituency	24	23	31
C03	G/PR-individual user accountability	25	24	20
B04	G/A-disaster recovery testing	26	25	32
C06	G/PR/TA-troubleshooting ITS problems	27	28	21
A08	**G-agency ITS policy**	28	17	35
C01	TA/PR-access control and authentication	29	29	28
B05	G/A-emergency response capability	30	30	29
B07	**G/A-certification and accreditation**	31	34	23
B06	G/A-independent security verification reviews	32	31	28
C02	TA/G-public access by client populations	33	33	27
B08	G/A-comprehensive personnel security program	34	32	32

TABLE APX(Q)-1
RANKING OF IMPORTANCE OF CANDIDATE NEEDS AMONG ALL RESPONDENTS AND SELECTED GOVERNMENT GRADES

Need No.	Candidate Need	All	13/14	15/SES
A04	P-putting ethics in OPM regs	35	35	34
C05	PR/S-satisfying (inter)national criteria	36	36	36

APPENDIX R
DIFFERENCES IN RANKINGS OF IMPORTANCE OF CANDIDATE NEEDS AMONG ALL RESPONDENTS AND SELECTED GOVERNMENT GRADES

(Note: In the table, for "*A* vs. *B*," a positive number indicates that *B* was rated more important than *A*, and a negative number indicates that *B* was rated less important that A.)

KEY TO TYPE OF CANDIDATE SECURITY NEED: A=assistance; G=guidance; P=policy; PR=products; S=standards; TA=technical approaches; TI=technical information

TABLE APX(R)-1
DIFFERENCES IN RANKINGS OF IMPORTANCE OF CANDIDATE NEEDS AMONG ALL RESPONDENTS AND SELECTED GOVERNMENT GRADES

Need No.	Candidate Need	All	Diff. All vs. 13/14	Diff. All vs. 15/SES	Diff. 13/14 vs. 15/SES
C10	S/G/TA/PR-LANs	1	0	-1	-1
C11	G/PR/TI-linking PCs/LANs/MFs in 1 ITS architecture	2	0	1	1
C14	G-database security	3	-1	-1	0
A05	P-ITS in system development life cycle	4	-1	1	2
B02	G/A-contingency and disaster recovery plans	5	-1	-3	-2
C13	G/TA-secure dial-in and laptops	6	-3	1	4
A03	P/G/TR-executive/mgt SA&T	7	-3	-2	1
A09	**G/S-defining sensitive systems**	8	0	-11	-11
A10	**G-developing security plans**	9	6	-13	-19
B01	G/PR/A-risk analysis	10	3	-5	-8
C12	**G-integrating open system products**	11	-15	5	20
A06	P-collection, dissemination, sharing	12	0	5	5

Appendix R

TABLE APX(R)-1
DIFFERENCES IN RANKINGS OF IMPORTANCE OF CANDIDATE NEEDS AMONG ALL RESPONDENTS AND SELECTED GOVERNMENT GRADES

Need No.	Candidate Need	All	Diff. All vs. 13/14	Diff. All vs. 15/SES	Diff. 13/14 vs. 15/SES
A01	P/G-integrating ITS policies and directives	13	-7	-3	4
B09	G/PR/A/materials-Security Awareness and Training	14	3	3	0
D01	**Clearinghouse of ITS information**	15	0	-10	-10
A07	P-emergency response capability	16	-6	2	8
C07	G/PR-EDI, PKE, DS, and elec. authentication	17	-2	5	7
A02	P-owner of sensitive systems	18	4	8	4
A11	**G-management-level ITS planning**	19	3	-11	-14
B03	G/TA/A-impact of security violations	20	-1	2	3
C08	TA/PR-ITS in s/w development and s/w engineering	21	3	8	5
C02	G/S-minimum controls for sensitivity levels	22	9	5	-4
C09	TI-computer security tools (evaluations)	23	-4	-1	3
D02	Better flow of info from NIST to constituency	24	1	-7	-8
C03	G/PR-individual user accountability	25	1	5	4
B04	G/A-disaster recovery testing	26	1	-7	-8
C06	G/PR/TA-troubleshooting ITS problems	27	-1	6	7
A08	**G-agency ITS policy**	28	11	-7	-18
C01	TA/PR-access control and authentication	29	0	3	3

TABLE APX(R)-1
DIFFERENCES IN RANKINGS OF IMPORTANCE OF CANDIDATE NEEDS AMONG ALL RESPONDENTS AND SELECTED GOVERNMENT GRADES

Need No.	Candidate Need	All	Diff. All vs. 13/14	Diff. All vs. 15/SES	Diff. 13/14 vs. 15/SES
B05	G/A-emergency response capability	30	0	1	1
B07	**G/A-certification and accreditation**	31	-3	8	11
B06	G/A-independent security verification reviews	32	1	4	3
C02	TA/G-public access by client populations	33	0	6	6
B08	G/A-comprehensive personnel security program	34	2	2	8
A04	P-putting ethics in OPM regs	35	0	1	1
C05	PR/S-satisfying (inter)national criteria	36	0	0	0

APPENDIX S
AVERAGE IMPORTANCE AND IMMEDIACY VALUES OF CANDIDATE NEEDS IN DESCENDING ORDER BY AVERAGE IMPORTANCE

The table below presents average importance and average immediacy values for each of the candidate needs. They are presented in descending order by average importance. Note: The larger the importance value, the more important the candidate need as reported by respondents. The smaller the immediacy value, the shorter the time frame in which that candidate need is wanted by respondents (i.e., the more urgent). (See Appendix W for a summary of the measures of dispersion for the data in this table.)

KEY TO TYPE OF CANDIDATE SECURITY NEED: A=assistance; G=guidance; P=policy; PR=products; S=standards; TA=technical approaches; TI=technical information

TABLE APX(S)-1
AVERAGE IMPORTANCE AND IMMEDIACY VALUES OF CANDIDATE NEEDS IN DESCENDING ORDER BY AVERAGE IMPORTANCE

Need No.	Candidate Need	Average Import.	Average Immed.
C10	S/G/TA/PR-LANs	3.73	1.54
C11	G/PR/TI-linking PCs/LANs/MFs in 1 ITS architecture	3.67	1.58
C14	G-database security	3.46	1.72
A05	P-ITS in system development life cycle	3.38	1.83
B02	G/A-contingency and disaster recovery plans	3.33	1.76
C13	G/TA-secure dial-in and laptops	3.32	1.80
A03	P/G/TR-executive/mgt SA&T	3.29	1.77
A09	G/S-defining sensitive systems	3.29	1.76
A10	G-developing security plans	3.23	1.85
B01	G/PR/A-risk analysis	3.22	1.79
C12	G-integrating open system products	3.22	2.00

TABLE APX(S)-1
AVERAGE IMPORTANCE AND IMMEDIACY VALUES OF CANDIDATE NEEDS IN DESCENDING ORDER BY AVERAGE IMPORTANCE

Need No.	Candidate Need	Average Import.	Average Immed.
A06	P-collection, dissemination, sharing	3.21	1.95
A01	P/G-integrating ITS policies and directives	3.21	1.84
B09	G/PR/A/materials-security awareness and trng.	3.19	1.85
D01	Clearinghouse of ITS information	3.18	1.98
A07	P-emergency response capability	3.15	1.84
C07	G/PR-EDI, PKE, DS, and elec. authentication	3.14	2.06
A02	P-owner of sensitive systems	3.13	1.77
A11	G-management-level ITS planning	3.12	1.86
B03	G/TA/A-impact of security violations	3.12	1.97
C08	TA/PR-ITS in s/w development and s/w engineering	3.09	2.03
C04	G/S-minimum controls for sensitivity levels	3.09	1.89
C09	TI-computer security tools (evaluations)	3.07	1.99
D02	Better flow of info from NIST to constituency	3.06	1.94
C03	G/PR-individual user accountability	3.02	1.99
B04	G/A-disaster recovery testing	3.01	2.01
A08	G-agency ITS policy	3.00	1.97
C06	G/PR/TA-troubleshooting ITS problems	3.00	2.05
C01	TA/PR-access control and authentication	2.97	1.97
B05	G/A-emergency response capability	2.95	2.02
B07	G/A-certification and accreditation	2.90	2.07
B06	G/A-independent security verification reviews	2.86	2.13
C02	TA/G-public access by client populations	2.82	2.14

TABLE APX(S)-1
AVERAGE IMPORTANCE AND IMMEDIACY VALUES OF CANDIDATE NEEDS IN DESCENDING ORDER BY AVERAGE IMPORTANCE

Need No.	Candidate Need	Average Import.	Average Immed.
B08	G/A-comprehensive personnel security program	2.74	2.13
A04	P-putting ethics in OPM regs	2.74	2.19
C05	PR/S-satisfying (inter)national criteria	2.41	2.41
Total		3.12	1.93

APPENDIX T
NORMALIZED AVERAGE IMPORTANCE AND IMMEDIACY VALUES OF CANDIDATE NEEDS IN DESCENDING ORDER BY AVERAGE IMPORTANCE

The table below presents the average importance and immediacy values from Appendix Z normalized by dividing each average importance by the mean average importance value (3.12) and by dividing each average immediacy by the mean average immediacy value (1.93). They are presented in descending order by average importance. Note: The *larger* the importance value, the more important the candidate need as reported by respondents. The *smaller* the immediacy value, the shorter the time frame in which that candidate need is wanted by respondents (i.e., the more urgent).

KEY TO TYPE OF CANDIDATE SECURITY NEED: A=assistance; G=guidance; P=policy; PR=products; S=standards; TA=technical approaches; TI=technical information

TABLE APX(T)-1
NORMALIZED AVERAGE IMPORTANCE AND IMMEDIACY VALUES OF CANDIDATE NEEDS IN DESCENDING ORDER BY AVERAGE IMPORTANCE

Need No.	Candidate Need	Norm. Average Import.	Norm. Average Immed.
C10	S/G/TA/PR-LANs	1.20	0.80
C11	G/PR/TI-linking PCs/LANs/MFs in 1 ITS architecture	1.19	0.82
C14	G-database security	1.14	0.89
A05	P-ITS in system development life cycle	1.10	0.95
B02	G/A-contingency and disaster recovery plans	1.08	0.91
C13	G/TA-secure dial-in and laptops	1.07	0.93
A03	P/G/TR-executive/mgt SA&T	1.06	0.92
A09	G/S-defining sensitive systems	1.06	0.91
A10	G-developing security plans	1.06	0.96

TABLE APX(T)-1
NORMALIZED AVERAGE IMPORTANCE AND IMMEDIACY VALUES OF CANDIDATE NEEDS IN DESCENDING ORDER BY AVERAGE IMPORTANCE

Need No.	Candidate Need	Norm. Average Import.	Norm. Average Immed.
B01	G/PR/A-risk analysis	1.04	0.93
C12	G-integrating open system products	1.04	1.04
A06	P-collection, dissemination, sharing	1.03	1.01
A01	P/G-integrating ITS policies and directives	1.02	0.96
B09	G/PR/A/materials-security awareness and trng.	1.02	0.96
D01	Clearinghouse of ITS information	1.02	1.03
A07	P-emergency response capability	1.01	0.96
C07	G/PR-EDI, PKE, DS, and elec. authentication	1.01	1.07
A02	P-owner of sensitive systems	1.01	0.92
A11	G-management-level ITS planning	1.01	0.97
B03	G/TA/A-impact of security violations	1.00	1.02
C08	TA/PR-ITS in s/w development and s/w engineering	1.00	1.05
C04	G/S-minimum controls for sensitivity levels	0.98	0.96
C09	TI-computer security tools (evaluations)	0.98	1.03
D02	Better flow of info from NIST to constituency	0.97	1.01
C03	G/PR-individual user accountability	0.96	1.03
B04	G/A-disaster recovery testing	0.94	1.04
A08	G-agency ITS policy	0.95	0.97
C06	G/PR/TA-troubleshooting ITS problems	0.93	1.06
C01	TA/PR-access control and authentication	0.94	1.02
B05	G/A-emergency response capability	0.93	1.05
B07	G/A-certification and accreditation	0.92	1.07

TABLE APX(T)-1
NORMALIZED AVERAGE IMPORTANCE AND IMMEDIACY VALUES OF CANDIDATE NEEDS IN DESCENDING ORDER BY AVERAGE IMPORTANCE

Need No.	Candidate Need	Norm. Average Import.	Norm. Average Immed.
B06	G/A-independent security verification reviews	0.91	1.11
C02	TA/G-public access by client populations	0.89	1.11
B08	G/A-comprehensive personnel security program	0.89	1.11
A04	P-putting ethics in OPM regs	0.85	1.14
C05	PR/S-satisfying (inter)national criteria	0.74	1.25
Total		1.00	1.00

APPENDIX U
VARIATIONS IN AVERAGE IMPORTANCE RATINGS OF CANDIDATE NEEDS IN DESCENDING ORDER BY AVERAGE IMPORTANCE

In order to examine the significance of the differences among average importance ratings, the number of standard deviations from the mean and the percentage of importance responses that rated as either highly important or very highly important were calculated for each candidate need. The results are shown in the following table.

KEY TO TYPE OF CANDIDATE SECURITY NEED: A=assistance; G=guidance; P=policy; PR=products; S=standards; TA=technical approaches; TI=technical information

TABLE APX(U)-1
VARIATIONS IN AVERAGE IMPORTANCE RATINGS OF CANDIDATE NEEDS IN DESCENDING ORDER BY AVERAGE IMPORTANCE

Nd. No.	Candidate Need	Avg. Import.	Norm. Avg. Import.	No. of Std Dv. fr Mean	Perct. High or Very High Import.
C10	S/G/TA/PR-LANs	3.73	1.20	2.49	66.1
C11	G/PR/TI-linking PCs/LANs/MFs in 1 ITS arch	3.67	1.19	2.24	61.2
C14	G-database security	3.46	1.14	1.39	52.7
A05	P-ITS in system development life cycle	3.32	1.10	1.06	44.2
B02	G/A-contingency and disaster recovery plans	3.33	1.08	0.86	46.4
C13	G/TA-secure dial-in and laptops	3.32	1.07	.0.82	49.6
A03	P/G/TR-executive/mgt SA&T	3.29	1.06	0.69	42.9

TABLE APX(U)-1
VARIATIONS IN AVERAGE IMPORTANCE RATINGS OF CANDIDATE NEEDS IN DESCENDING ORDER BY AVERAGE IMPORTANCE

Nd. No.	Candidate Need	Avg. Import.	Norm. Avg. Import.	No. of Std Dv. fr Mean	Perct. High or Very High Import.
A09	G/S-defining sensitive systems	3.29	1.06	0.69	43.3
A10	G-developing security plans	3.23	1.06	0.45	41.5
B01	G/PR/A-risk analysis	3.22	1.04	0.41	42.0
C12	G-integrating open system products	3.22	1.04	0.41	39.7
A06	P-collection, dissemination, sharing	3.21	1.03	0.37	38.4
A01	P/G-integrating ITS policies and directives	3.21	1.02	0.37	38.4
B09	G/PR/A/materials-Security Awareness and Trg.	3.19	1.02	0.24	36.2
D01	Clearinghouse of ITS information	3.18	1.02	0.24	36.2
A07	P-emergency response capability	3.18	1.01	0.12	42.0
C07	G/PR-EDI, PKE, DS, and elec. authentication	3.14	1.01	0.08	35.7
A02	P-owner of sensitive systems	3.13	1.01	0.04	37.9
A11	G-management-level ITS planning	3.12	1.01	0.00	36.6

TABLE APX(U)-1
VARIATIONS IN AVERAGE IMPORTANCE RATINGS OF CANDIDATE NEEDS IN DESCENDING ORDER BY AVERAGE IMPORTANCE

Nd. No.	Candidate Need	Avg. Import.	Norm. Avg. Import.	No. of Std Dv. fr Mean	Perct. High or Very High Import.
B03	G/TA/A-impact of security violations	3.12	1.00	0.00	36.6
C08	TA/PR-ITS in s/w development and s/w engrg	3.09	1.00	-0.12	38.4
C04	G/S-minimum controls for sensitivity levels	3.09	0.98	-0.12	36.6
C09	TI-computer security tools (evaluations)	3.07	0.98	-0.20	29.0
D02	Better flow of info from NIST to constituency	3.06	0.97	-0.24	33.5
C03	G/PR-individual user accountability	3.02	0.96	-0.41	31.7
B04	G/A-disaster recovery testing	3.09	0.94	-0.45	31.3
A08	G-agency ITS policy	3.00	0.95	-0.49	33.5
C06	G/PR/TA-troubleshooting ITS problems	3.00	0.94	-0.49	29.0
C01	TA/PR-access control and authentication	2.97	0.94	-0.61	30.8
B05	G/A-emergency response capability	2.95	0.93	-0.69	30.4
B07	G/A-certification and accreditation	2.90	0.92	-0.90	29.0

TABLE APX(U)-1
VARIATIONS IN AVERAGE IMPORTANCE RATINGS OF CANDIDATE NEEDS IN DESCENDING ORDER BY AVERAGE IMPORTANCE

Nd. No.	Candidate Need	Avg. Import.	Norm. Avg. Import.	No. of Std Dv. fr Mean	Perct. High or Very High Import.
B06	G/A-independent security verification reviews	2.86	0.91	-1.06	27.2
C02	TA/G-public access by client populations	2.82	0.89	-1.22	29.5
B08	G/A-comprehensive personnel security pgm.	2.74	0.89	-1.55	25.4
A04	P-putting ethics in OPM regs	2.74	0.85	-1.55	21.4
C05	PR/S-satisfying (inter)national criteria	2.41	0.74	-2.41	13.8
Total		3.12	1.00	0	37.2