NUREG/BR-0166

United States
Nuclear Regulatory Commission

Instructions for Preparing Security Plans for Local Area Networks in Compliance With OMB Bulletin No. 90–08

February 1992

Prepared by
National Institute of Standards and Technology
Office of Management and Budget
U.S. Nuclear Regulatory Commission
Office of Information Resources Management

NUREG/BR-0166

United States
Nuclear Regulatory Commission

Instructions for Preparing Security Plans for Local Area Networks in Compliance With OMB Bulletin No. 90–08

February 1992

Prepared by
National Institute of Standards and Technology
Office of Management and Budget
U.S. Nuclear Regulatory Commission
Office of Information Resources Management

ABSTRACT

This document provides guidelines for U.S. Nuclear Regulatory Commission managers, other staff members, and contractors who are responsible for developing computer security plans for local area networks. It was developed to supplement Office of Management and Budget Bulletin No. 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information." Agency managers, network administrators, system users, and security officers should be included when planning for security to ensure that all areas of concerns are considered.

Contents

PREFACE

This document provides guidelines for U.S. Nuclear Regulatory Commission managers, other staff members, and contractors who are responsible for preparing security plans for local area networks. It was developed by the National Institute of Standards and Technology to supplement the guidance in Office of Management and Budget (OMB) Bulletin No. 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information," which mandates security plans but does not address local area networks. The guidelines on how to prepare a security plan for local area networks are to be used by the NRC staff and contractors along with OMB Bulletin No. 90-08. The objectives of these guidelines are to help agency personnel and contractors

- understand the process for preparing a network security plan in conjunction with OMB Bulletin No. 90-08

- reduce the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of information in NRC networked computer systems

- understand the nature and extent of sensitive information systems and the security requirements for such systems

- understand the adequacy of the administrative, management, and technical approaches used in protecting sensitive systems in networked environments

- understand the responsibilities and accountability for the security of sensitive systems in networked environments

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

Instructions For Preparing Security Plans For Local Area Networks In Compliance With OMB Bulletin No. 90-08

This document is to be used as a companion document to Office of Management and Budget (OMB) Bulletin No. 90-08,"Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information," when preparing a computer security plan for a local area network (LAN). A sample LAN security plan is included as Appendix A to this document; OMB Bulletin No. 90-08 is reproduced in Appendix B.

I. System Identification

This section of the LAN security plan should contain basic identifying information.

A. Responsible Organization

Name the organization that is responsible for ensuring network continuity. State if this network is run by a contractor or State agency.

B. System Name/Title

The title should be meaningful and should describe the system, keeping in mind the organization's mission. This title is not always what users or operators call the system (e.g., the LAN). It should be descriptive of the kind of processing that is done (e.g., personnel/payroll LAN).

C. System Category

Most networks will be categorized as general support systems; however, some networks can be major application systems.

Major Application: A major application system performs a clearly defined function for which there are readily identifiable security considerations and needs.

- Is the network dedicated to one application? Is the network managed as a part of the application?

General Support System: A general support system consists of hardware and software that provide general automated data processing (ADP) or network support for a variety of users and applications.

- Does this network provide general ADP support for a variety of users and applications? If none of the applications are sensitive, perhaps the support system itself may be considered sensitive.

D. System Operational Status

Describe the operational status of the network (i.e., operational, under development, or undergoing a major modification).

E. General Description/Purpose

Provide a brief description of the function and purpose of this network. Include a concise description of the type of information that is handled by this network.

- What kind of information does this network contain or transmit (e.g., project data, personnel data)?
- What is the nature of the applications (i.e., what is this network used for)?
- Have the security requirements been coordinated between the users and network management (i.e., has the network security officer polled the users to determine what types of security requirements are needed)?

F. System Environment and Special Considerations

Provide a general description of the technical system. Include environmental concerns. Describe the operating and applications software.

- How is the operating and applications software licensed (i.e., site wide, multiple user, single user)?
- Is the network located in an office building, in a computing facility, or off site?
- Are there any special conditions such as high-traffic areas, water damage, or earthquakes? Is this network located in a harsh or overseas environment?
- Is this network connected to any public lines or networks? Is there any dial-up capability?
- What equipment does this network consist of (e.g., personal computers, minicomputers, mainframes)?
- What is the network operating system? What are the software packages that run on this network? Are these packages off-the-shelf or custom-made software?
- Who are the users of this network (i.e., is it used within the agency, between agencies, by contractors, by the general public, by foreign nationals)?

- Are there any other types of interfaces with other Federal and non-Federal systems?

G. Information Contact(s)

Provide the name, title, organization, and telephone number of one or more persons designated to be the point of contact for this network. This contact must be knowledgeable enough to provide additional information regarding the use and security of this network if needed (e.g., systems administrator, security officer).

II. Sensitivity of Information Handled

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

A. Applicable Laws or Regulations Affecting the System

Examples are the Privacy Act and the Financial Managers Integrity Act.

B. General Description of Information Sensitivity

The information stored on and transmitted by this network should be addressed in accordance with OMB Bulletin No. 90-08.

A system may need protection for one or more of the following reasons:

- Confidentiality: The need to protect information from intentional and unintentional disclosure (e.g., personal data, proprietary information).
  - Does this network store or transmit information such as Social Security numbers, medical information, financial information, time release critical information?
- Integrity: The need to protect information from intentional and unintentional modification (e.g., financial information, scientific research information).
  - Does this network store or transmit life-threatening information (e.g., air traffic control information, hazardous weather conditions)?
  - Does this network store or transmit such information that if its accuracy were not protected, the agency's mission could not be accomplished?
  - Is this network used for scientific or medical research where the information needs to be as accurate as possible (e.g., pharmaceutical testing information, cancer research data)?
- Availability: The need to protect information from intentional and unintentional loss (e.g., air traffic control information, payment dissemination).
  - Does this network store or transmit information that needs to be available in a timely manner (e.g.,census information, air traffic control information)?
  - Would the unavailability of this network cause a loss of life, monetary loss, failure of the agency's mission, or embarrassment to the Government?
  - How long can this office function without the use of this network?

For each category (confidentiality, integrity, and availability), indicate a protection requirement of high, medium, or low.

III. System Security Measures

This section should contain a description of the control measures. To ascertain which controls and procedures are needed to protect this network, threats and vulnerabilities need to be assessed.

A. Risk Assessment and Management

Risk assessment and management are crucial elements of the security planning process.

- Has a risk analysis of this network ever been performed? If so, describe the methodology used.

B. Applicable Guidance

Provide a list of specific standards or other guidance that was used in the design, implementation, or operation of the protective measures used on this network.

- What standards or guidelines were used in the design, implementation, or operation of the protective measures that are used on this network (e.g., encryption keys, data authentication, key management, NRC computer security policy documents)?
- Was any policy, guideline, or standard developed by the NRC used in the implementation, design, or operation of the network security measures?

C. Security Control Measures

There are two sets of controls: one for major applications and one for general ADP support systems. Because networks tend to be general support systems, Section F will most likely be used. If the network is a major application, use Section E. State whether the controls are in place, planned, in place and planned, or not applicable. For the planned controls, give the date when these controls will be implemented. It is also helpful to the network manager and users to describe these control measures.

D. Security Control Measures Status

For each of the control measures in Sections E and F, specify if it is (1) in place, (2) planned, (3) in place and planned, or (4) not applicable.

E. Security Control Measures for Major Applications

1. Management Controls

These controls are used for the overall management of the network as a major application. They include authorization, personnel screening, risk management, and assignment of security responsibility.

a. *Assignment of Security Responsibility*

The assignment of security responsibility is important to ensure that security is considered. The person assigned this responsibility should be responsible for all aspects of the security of the network.

- Who is responsible if something goes wrong? Has the responsibility for the security of this network been assigned? This responsibility should NOT be assigned to the network administrator. Often if the network administrator and security officer are the same, security is overlooked to keep the network running.

b. *Personnel Screening*

Personnel screening should be in place. This screening should include making sure only personnel with a need to know have access to the network.

- Have personnel had background checks?

- Does anyone who can access the network need to be screened?

2. Development/Implementation Controls

These controls ensure that protection is built into the network, especially during network development.

a. *Security Specifications*

Security specifications should be in place for the appropriate technical, administrative, physical, and personnel security required for networks.

- Are the appropriate technical specifications in place for this network?

- Do these technical specifications include security for shared file access such as file locking and record locking?

- Is a password management system in place?

- Are controls in place for personnel security? Are appropriate personnel procedures and policies in place?

b. *Design Review and Testing*

A design review and systems test should be completed before this major application network is in operation. The review and test are needed to ensure that the major application network meets the security specifications. Full documentation of this design review and test should be kept and maintained.

- Have a design review and test been completed? Do the results show that the major applica-tion network meets the security specifications required?

c. *Certification*

Networks should be certified in accordance with OMB Bulletin No. 90-08.

- Has management authorized this network for sensitive processing? This may include any constraints placed on processing, such as no processing during nonwork hours or no use of dial-up lines.

3. Operational Controls

These controls include the day-to-day procedures and mechanisms that are used to protect the operational application networks.

a. *Physical and Environmental Protection*

These controls provide for the physical and environmental protection of the network, including all physical protection devices such as fire extinguishers, locks, or video cameras.

- Are controls in place to protect this network against physical and environmental threats and hazards?
- Is this network housed in an office building with doors that can be locked? Are any switches or terminals accessible to unauthorized personnel?
- Is there 24-hour guard service?
- Is proper firefighting equipment available?
- Are proper water detection devices along with means to eliminate excess water available?
- Are fire, heat, and smoke detectors in place?
- Are uninterruptible power supplies or electrical surge protectors available?

b. *Production, I/O [Input/Output] Controls*

These controls provide for the proper handling, processing, storage, and disposal of the input and output of the network.

- Are controls in place to manage the input and output? This includes the storage and disposal of printouts and floppy diskettes or other media on which information is stored or data screening.
- Are input and output media properly labeled (e.g., labels stating "project x,y,z" or "sensitive")?

c. *Emergency, Backup, and Contingency Planning*

These controls include the measures that are to be used to ensure continuity of support in the event of a network failure.

- Are the appropriate emergency, backup, and contingency plans in place for this network?
- Are these plans readily available for the network manager and users in case of an emergency? These plans should ensure the continuity of support in the event of a network failure.
- Is there an alternative network that could be used in case of an emergency?
- Can the duties of this office be performed manually in case of an emergency?

d. *Audit and Variance Detection*

These controls allow management to conduct independent reviews of records and activities to test the adequacy of controls and to detect and react to departures from established policies, rules, and procedures. Variance detection checks for anomalies in such items as numbers and types of transactions and volume and dollar thresholds, and other deviations from standard activity profiles.

- Are there controls that will allow management to conduct an independent review of the systems records and activities? The purpose of this review should be to test the adequacy of network controls and to detect and react to departures from established procedures, policies, and rules.
- Are there sign-in and sign-out logs for those who have physical access to the network server?
- Are job request forms necessary? If so, are they used?
- Is there a mechanism to monitor the network load and number of access attempts?
- Is there any software residing on this network that monitors for viruses or other anomalies?

e. *Application Software Maintenance Controls*

These controls are used to monitor application software installation and updates. They ensure that the software functions as expected and that a historical record of application system changes is maintained.

- Are controls in place to monitor the application software updates?

- Is there a software configuration policy? If so, who authorizes the software changes and updates?

- Is a record kept and maintained regarding the software changes and updates? If so, is this record available to the appropriate personnel when it is needed?

- Are virus-protection products used to check if application software has been modified?

f. *Documentation*

This section should be completed in accordance with OMB Bulletin No. 90-08.

- Are there descriptions of the hardware and software, policies, and procedures related to the computer security of the network? These should include backup and contingency plans for the network and a description of the operator procedures.

- Are there descriptions of the network layout, software, hardware, and configuration or cable charts?

- Are there descriptions of the end-user procedures regarding proper handling of sensitive data?

- Are these descriptions readily available to all who need access to them?

- Are there any maintenance contracts regarding this network? Are they accessible to the personnel who need them?

4. Security Awareness and Training

a. Security Awareness and Training Measures

This section should be completed in accordance with OMB Bulletin No. 90-08.

- Is a security awareness and training course for users, technical staff, and managers in place?

- What is included in this training course?

- Does this training address specific network issues, such as the protection of passwords?

- How often is this course offered?

- Do all employees have to attend this course periodically?

- Is security covered in any other ADP training such as WordPerfect, dBase, or Lotus 1,2,3?

5. Technical Controls

This section should be completed in accordance with OMB Bulletin No. 90-08.

Most of the following controls are found within the network operating system and should be described in the network operating system documentation.

a. *User Identification and Authentication*

These controls are used to verify the identity of a station, originator, or individual before allowing access to the network. They are the basis for authorization and access controls.

- Is user identification required to access this network?

- Does this network pass this identification to other networks that are connected?

- Are passwords, tokens, or other mechanisms used to authenticate the identity of a user (e.g., encryption keys, fingerprints, voice or signature authentication) before access to the network is granted?

b. *Authorization/Access Controls*

These controls are used to detect and/or permit only authorized access to or within the network.

- Does the operating system offer controls to restrict access to the operating system? If not, are any controls developed by the NRC in place?

- Are any hardware or software features used to detect and/or permit only authorized access to or within the system used (e.g., access lists)?

- Are there limits on access to computer programming resources?

- Does the operating system have built-in authorization and access controls that can be adjusted to allow or disallow reading, writing, or executing files and programs?

c. *Data Integrity/Validation Controls*

These controls protect the operating system, application system, and information from alteration or destruction.

- Are any controls in place that provide message authentication?

d. *Audit Trails and Journaling*

These controls provide monitoring and recording capabilities to retain a chronologicr l record of system activities.

- Is there an audit trail mechanism to record and monitor network activity (e.g., system log)?
- Can this mechanism be used to reconstruct the activities of the network when a problem is detected?

6. Complementary Controls Provided by Support Systems

F. Security Control Measures for General Support Systems

1. Management Controls

These controls are used for the overall management of the network. They include authorization, personnel screening, risk management, and assignment of security responsibility.

a. *Assignment of Security Responsibility*

The assignment of security responsibility is important to ensure continuity of network operations. The person assigned this responsibility should be responsible for all aspects of the security of the network.

- Who is responsible if something goes wrong? Has the responsibility for the security of this network been assigned? This responsibility should NOT be assigned to the network administrator. Often if the network administrator and security officer are the same, security is overlooked to keep the network running.
- Is there a checksum capability within the operating system that allows files to be checked after transmission to ensure the correct number of bytes was transferred?
- Is an error-checking or error-correcting technique used?
- Is nonrepudiation available?

b. *Risk Analysis*

Many risk analyses do not address networks directly.

- Did the risk analysis that was used address the network directly?

c. *Personnel Screening*

Personnel screening should be in place. This screening should include making sure only personnel with a need to know have access to the network.

- Have personnel had background checks?
- Does anyone who can access the network need to be screened?

2. Acquisition/Development/Installation Controls

These controls ensure that adequate security is built into and maintained in the network to minimize the damage that could occur as a result of threats and vulnerabilities.

a. *Acquisition Specifications*

Security should be included in the acquisition specifications for a network. It is less expensive to have security built into the network from the beginning. When adding security to an already existing network, many vulnerabilities may be overlooked.

- Was security included in the life cycle of the development model?
- Have the appropriate specifications been considered in the technical, administrative, physical, and personnel security areas?
- Do all the contracts for the procurement of computer hardware, software, and services for this network include a

specification for security requirements?

b. *Accreditation/Certification*

Networks should be accredited and certified in accordance with OMB Bulletin No. 90-08.

- Has management authorized this network for processing sensitive information? This may include any constraints placed on processing, such as no processing during nonworking hours or no use of dial-up lines.

3. Operational Controls

These controls should include physical and environmental protection, emergency backup systems, contingency planning, audit and variance detection, maintenance of application software, documentation, and a periodic check for viruses.

a. *Physical and Environmental Protection*

These controls provide for the physical and environmental protection of the network, including all physical protection devices such as fire extinguishers, locks, or video cameras.

- Are controls in place to protect this network against physical and environmental threats and hazards?

- Is this network housed in an office building with doors that can be locked. Are any switches or terminals accessible to unauthorized personnel?

- Is there 24-hour guard service?

- Is proper firefighting equipment available?

- Are proper water detection devices along with means to eliminate excess water available?

- Are fire, heat, and smoke detectors in place?

- Are uninterruptible power supplies or electrical surge protectors available?

b. *Production, I/O [Input/Output] Controls*

These controls provide for the proper handling, processing, storage, and disposal of the input and output of the network.

- Are controls in place to manage the input and output? This includes the storage and disposal of printouts and floppy diskettes or other media on which information is stored or data screening.

- Are input and output media properly labeled (e.g., labels stating "project x,y,z" or "sensitive")?

c. *Emergency, Backup, and Contingency Planning*

These controls include the measures that are to be used to ensure continuity of support in the event of a network failure.

- Are the appropriate emergency, backup, and contingency plans in place for this network?

- Are these plans readily available for the network manager and users in case of an emergency? These plans should ensure the continuity of support in the event of a network failure.

- Is there an alternative network that could be used in case of an emergency?

- Can the duties of this office be performed manually in case of an emergency?

d. *Audit and Variance Detection*

These controls allow management to conduct independent reviews of records and activities to test the adequacy of controls and to detect and react to departures from established policies, rules, and procedures. Variance detection checks for anomalies in such items as numbers and types of transactions and volume and dollar thresholds, and other deviations from standard activity profiles.

- Are there controls that will allow management to conduct an independent review of the systems records and activities? The purpose of this review should be to test the adequacy of network controls and to detect and react to departures from the established procedures, policies, and rules.

- Are there sign-in and sign-out logs of those who have physical access to the network server?

- Are job request forms necessary? If so, are they used?

- Is there a mechanism to monitor the network load and number of access attempts?

- Is there any software residing on this network that monitors for viruses?

e. *Hardware and System Maintenance Controls*

This section should be completed in accordance with OMB Bulletin No. 90-08.

- Are controls in place to monitor the installation of software updates? These controls include keeping a historical record of the system changes and ensuring that only authorized software is installed on the network.

- Is there a record of all installations and modifications of software and hardware?

- Is the software and hardware tested before the real-time use of the system goes into effect?

f. *Documentation*

This section should be completed in accordance with OMB Bulletin No. 90-08.

- Are there descriptions of the hardware and software, policies, and procedures related to the computer security of the network? These should include backup and contingency plans for the network and a description of the operator procedures.

- Are there descriptions of the network layout, software, hardware, and configuration or cable charts?

- Are these descriptions readily available to all who need access to them?

- Are there any maintenance contracts regarding this network? Are they accessible to the personnel who need them?

4. Security Awareness and Training

a. *Security Awareness and Training Measures*

This section should bc completed in accordance with OMB Bulletin No. 90-08.

- Is a security awareness and training course for users, technical staff, and managers in place?

- What is included in this training course?

- Does this training address specific network issues, such as the protection of passwords?

- How often is this course offered?

- Do all employees have to attend this course periodically?

5. Technical Controls

Most of the following controls are found within the network operating system and should be described in the network operating system documentation.

a. *User Identification and Authentication*

These controls are used to verify the identity of a station, originator, or individual before allowing access to the network. They are the basis for authorization and access controls.

- Is user identification required to access this network?

- Does this network pass this identification to other networks that are connected?

- Are passwords, tokens, or other mechanisms used to authenticate the identity of a user (e.g., encryption keys, fingerprints, voice or signature authentication) before access to the work is granted?

b. *Authorization/Access Controls*

These controls are used to detect and/or permit only authorized access to or within the network.

- Does the operating system offer controls to restrict access to the operating system? If not, are any controls developed by the NRC in place?

- Are any hardware or software features used to detect and/or permit only authorized access to or within the system used (e.g., access lists)?

- Are there limits on access to computer programming resources?

- Does the operating system have built-in authorization and access controls that can be adjusted to allow or disallow reading, writing, or executing files and programs?

c. *Integrity Controls*

These controls protect the operating system, application system, and information from alteration or destruction.

- Are any controls in place that provide message authentication?

- Is there a checksum capability within the operating system that allows files to be checked after transmission to ensure the correct number of bytes was transferred?

- Is an error-checking or error-correcting technique used?

- Is nonrepudiation available?

d. *Audit Trail Mechanisms*

These controls provide monitoring and recording capabilities to retain a chronological record of system activities.

- Is there an audit trail mechanism to record and monitor network activity (e.g., system log)?

- Can this mechanism be used to reconstruct the activities of the network when a problem is detected?

e. *Confidentiality Controls*

These controls provide protection for data that must be held in confidence and protected from unauthorized disclosure. They may provide data protection at the user site, at the computer facility, in transit, or some combination of these.

- Is encryption used to ensure confidentiality during storage or transmission?

- Are any other technical means used to protect confidentiality?

6. Controls Over the Security of Applications

The security of each application that is processed on a support system could affect the security of all others processed on that same system.

- Is the manager of the network aware of the security requirements of the applications that are processed? The manager should understand the risk that each application represents to the overall system.

- Are the network users and applications owners aware of what the network does and does not do to protect sensitive data?

IV. Additional Comments

This section is intended for additional comments about the security of this network and any perceived need for guidance or standards.

- Is there anything else of importance about the security of this network that was not covered in the preceding sections?

- Is any additional security guidance or security standard needed that would ensure that this network operates more efficiently?

APPENDIX A

Sample Security Plan For A Local Area Network

APPENDIX A
SAMPLE SECURITY PLAN FOR A LOCAL AREA NETWORK

The following is a sample security plan for a local area network (LAN) that follows OMB Bulletin No. 90-08 and the guidelines developed by the National Institute of Standards and Technology. The following entries should be included in this security plan.

I. SYSTEM IDENTIFICATION

A. Responsible Organization

U.S. Nuclear Regulatory Commission
Branch: ____________
Office: ____________

B. System Name/Title

System A.

C. System Category

Major application.

D. System Operational Status

Operational.

E. General Description/Purpose

The immediate and primary continuing purpose of System A is to limit the consequences of incidents at nuclear power reactors. It is used to recommend to State and local authorities whatever actions may be necessary to protect the public and the environment. The NRC, through independent assessments and support where necessary, adds a safety factor to help ensure that the protective measures being recommended are adequate.

System A consists of three microcomputer-based subsystems: (1) LAN 1, (2) LAN 2, and (3) personal computer (PC) workstations.

LAN 1 includes workstations throughout the System A area. It is used to run models, exchange information, and send summary reports to other organizations. It also backs up LAN 2.

LAN 2 is the primary support for routine func ons at all hours in the System A area. It contains all of the programs needed by system A personnel to compile periodic summaries and plant status reports. The PC workstation subsystem comprises several stand-alone workstations within and outside the System A area that are not connected to the LAN.

F. System Environment and Special Considerations

LAN 1 and LAN 2 are fully contained within the System A area and require an access code on a keycard to open the door. All LAN servers are kept in a locked room that is closely monitored. Only authorized personnel are issued keys to the room.

G. Information Contact

John Doe, Chief, Office of __________, (xxx) xxx-xxxx

II. SENSITIVITY OF INFORMATION HANDLED

A. Applicable Laws or Regulations Affecting the System

Information maintained in this system is covered by the provisions of the Privacy Act of 1974, 5 U.S.C. 552a, and NRC's regulations in 10 CFR Part 9.

B. General Description of Information Sensitivity

Confidentiality of data—Primary concern

Integrity of data—Primary concern

Availability of data—Primary concern

C. Need for Protective Measures

The information that is stored on System A's PC workstations is personnel information, that is, employees' Social Security numbers, grades, addresses, telephone numbers, and birth dates. This type of information is considered sensitive. For this reason, the system is considered to be sensitive unclassified. No sensitive information is stored on the LAN. Sensitive information should NEVER be stored on the LAN.

D. Estimated Risk

Because of the sensitive information that is stored in System A, the estimated risk of disclosure with regard to integrity, availability, and confidentiality would be a primary concern.

E. Protection Requirement

The System A PCs and LANs must maintain "high" confidentiality and "high" integrity for all identifiers such as Social Security numbers, grades, birth dates, and home telephone numbers because unauthorized access could mean loss of privacy for incividuals. The System A LANs must maintain "high" availability because they support continuous organizational functions.

III. SYSTEM SECURITY MEASURES

A. Risk Assessment and Management

The National Institute of Standards and Technology (NIST) (formerly the National Bureau of Standards) performed a formal risk analysis of System A in 1985. The Office of Information Resources Management, Codes and Standards Section, performed a risk analysis of the system in 1990, using the Los Alamos Vulnerability Analysis Tool to determine the vulnerabilities in the system and ways to correct them.

B. Applicable Guidance

NRC Appendix 2301, "Security of Automated Information Systems," dated July 25, 1985, Part II, paragraph A.1, addresses the requirement for unclassified systems processing sensitive or sensitive unclassified data. The Privacy Act, mentioned in Section II.A, also applies. The Computer Security Act of 1987 does not apply.

C. Security Control Measures (According to OMB Circular No. A-130)

Specific control measures are in place for System A to ensure that management of the system is being monitored. These control measures adhere to the requirements specified in the Computer Security Act of 1987; OMB Circular No. A-130, Appendix III, "Management of Federal Information Resources"; and applicable Federal Information Processing Standards and Special Publications produced by NIST.

D. Security Control Measures Status

Specific management, operational, and technical measures that are in place, planned, in place and planned, or not applicable are described in Section E of this plan for System A.

E. Security Control Measures for Major Applications

1. Management Controls—In place

a. *Assignment of Security Responsibility*—In p'ace.

The duties of system security officer have been assigned to John Doe, Office of Supply, (xxx) xxx-xxxx. The duties of assistant security officer have been assigned to Jane Doe, Office of Supply, (xxx) xxx-xxxx.

b. *Personnel Screening*—In place.

All agency personnel involved in the use, design, development, operation, or maintenance of System A undergo a background investigation. In addition, agency personnel and contractors must meet the requirements for Federal employees and contractors found in Office of Personnel Management Federal Personnel Manual Chapters 731, 732, and 736.

2. Development/Implementation Controls—In place.

a. *Security Specifications*—In place where applicable.

Operational security requirements have been defined for system developers. System A and System B (backup to System A) are being completed under contracts that specify the requirements; System A is composed largely of off-the-shelf components, including software, that are selected and integrated to meet operational requirements.

b. *Design Review and Testing*—In place where applicable.

System A design reviews have been completed.

c. *Certification*—In place where applicable.

The Office of Information Resources Management has approved System A designs.

3. Operational Controls—In place.

a. *Physical and Environmental Protection*—In place.

Access to the System A area is controlled by keycard doors.

b. *Production, I/O [Input/Output] Controls*—Not applicable.

c. *Emergency, Backup and Contingency Planning*—In place.

Computer programs and data are backed up or are available at more than one location in the event of a localized problem. A tape backup is being installed on System A, because the system may, at times, contain information that is not duplicated elsewhere. Systems in the System A area are designed with either a system of workstation uninterruptible power supplies and mirrored external drives or mutual backup in the event of a workstation failure. A roof-mounted diesel generator automatically delivers power for equipment, telephones, and lighting if there is a major loss of power. In case of a more widespread problem, procedures to rely on paper forms and other communications that were used before computers were available are in place and have been tested. A complete contingency plan is being developed.

d. *Audit and Variance Detection*—In place.

Only one function of System A lends itself to "standard activity profiles." Costs, access times and duration, activities, and other audit factors are monitored by the office responsible for the commercial electronic message service used to support emergency response functions.

e. *Application Software Maintenance Controls*—In place.

System A software is standard for all users. One person approves functional modifications, and other designated persons implement and test the modifications to ensure that they do not have unintended operational effects. In addition, two persons are responsible for ensuring that any workstation will function as required at any time. The latest software versions are documented. Similar requirements apply to other System A subsystems.

f. *Documentation*—In place.

The Office of Information Resources Management (IRM) maintains security-related policies, standards, and other policies. The IRM LAN manager maintains LAN system documentation. IRM personnel maintain application documentation, user procedures, and a mailing list of persons to contact to address various problems.

4. Security Awareness and Training—In place.

Specific security measures that relate to specific applications are included with user procedures (e.g., changing passwords); these measures will be reviewed and improved as necessary on the basis of this security plan.

5. Technical Controls—In place.

a. *User Identification and Authentication*—In place.

LAN equipment requires an assigned account and six-character passwords for access to computer programs.

b. *Authorization/Access Controls*—In place.

System A data and programs can be changed only from a single workstation located in the LAN area. All LAN workstations can use only the programs for which a LAN manager has granted access.

c. *Data Integrity/Validation Controls*—In place.

System A data are checked during transmission. Computer programs are backed up using highquality, off-the-shelf software, and data from these programs are generally used only temporarily and stored on diskettes or tapes that are physically protected while the data are being used. Messages between the System A area and the rest of the world are stored on the protected computers of the commercial electronic message service or arrive via fax (hard copy) in the System A area. The procedure for exchanging messages in any medium requires authentication of the source and verification of certain data via telephone to a number arranged in advance.

d. *Audit Trails and Journaling*—In place.

LAN software maintains records of activities, as do the commercial data bases. The electronic message service also notifies any user if unsuccessful attempts have been made to log in.

6. Complementary Controls Provided by Support Systems—In place.

All users of System A who support daily activities receive regular specialized training tailored to their roles. One result is that users quickly spot anything that differs from what they have been trained to expect. Members of the staff who are responsible for System A development, maintenance, and training can then use their knowledge of and experience with the system to identify possible security problems.

F. Security Control Measures for General Support Systems

Not applicable. If the system is a general support system (a system used by many users in different locations within the same organization), the information called for in Section F of Appendix A to OMB Bulletin No. 90–08 and the NIST guidelines should be supplied instead of that called for in Section E.

IV. ADDITIONAL COMMENTS

Because both staff and computer security are involved, both the NRC Office of Security and the computer security staff in the Office of Information Resources Management will review this security plan.

APPENDIX B

OMB Bulletin No. 90-08, "Guidance For Preparation Of Security Plans For Federal Computer Systems That Contain Sensitive Information

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

July 9, 1990

THE DIRECTOR

OMB Bulletin No. 90-08

TO THE HEADS OF EXECUTIVE DEPARTMENTS AND ESTABLISHMENTS

SUBJECT: Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information

1. **Purpose**. The purpose of this Bulletin is to provide guidance to Federal agencies on computer security planning activities required by the Computer Security Act of 1987. This Bulletin supersedes OMB Bulletin No. 88-16, "Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information" (July 6, 1988).

2. **Authority**. The Computer Security Act of 1987 ("The Act") (P.L. 100-235), requires Federal agencies to identify each computer system that contains sensitive information and to prepare and implement a plan for the security and privacy of these systems. The Act further requires agencies to submit copies of those plans to the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) for advice and comment, and it makes such plans subject to OMB disapproval.

3. **Objectives of the Security Planning Process**. The security planning process is designed to reduce the risk and magnitude of harm that could result from the loss, misuses or unauthorized access to or modification of information in Federal computer systems. This process is intended to help agencies identify and assess:

   a. the nature and extent of sensitive information systems and the security requirements of such systems;

   b. the adequacy of the administrative, management, and technical approaches used in protecting sensitive systems;

   c. responsibilities and accountability for the security of sensitive systems; and

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

4. **Applicability.** This Bulletin applies to Federal agencies as defined in Section 3(b) of the Federal Property and Administrative Services Act of 1949, as amended. The Bulletin does not apply to agency operation of systems that contain classified information, systems involving intelligence activities, cryptologic activities related to national security, or direct command and control of military forces. The Bulletin also does not apply to equipment that is integral to a weapons system or direct fulfillment of military or intelligence missions (excluded by 10 U.S.C. 2315). In addition, it does not apply to mixed classified/unclassified systems, if such systems are always operated under rules for protecting classified information.

5. **Changes from OMB Bulletin No. 88-16.**

   a. This year's effort will focus on implementation of security plans.

   b. There will be site visits to the departments and agencies to discuss their computer security programs and identify and fix deficiencies in those programs.

   c. New security plans are not required for all systems. Plans are only required for new systems and those for which an acceptable plan was not previously reviewed.

   d. Guidance for preparing individual plans is revised and expanded based on last year's experience.

6. Action Required.

   a. Every agency must implement security plans for systems which contain sensitive information, incorporating appropriate advice and comment from NIST/NSA.

   b. Every agency must prepare a new computer security plan for each system that contains sensitive information, if:

      (1) the system is new or significantly modified; or

      (2) a plan for the system was not previously sent to NIST/NSA for advice and comment (particular emphasis should be on contractor, State, and local systems operated on behalf of the agency to perform a Federal function); or

      (3) staff members of NIST/NSA advised the agency they were unable to provide advice and comment on the previous plan for the system.

   These plans should be consistent with the format shown in Appendix A. Alternative formats may be used, provided they contain, at a minimum, the information described in Appendix A.

c. Every agency must establish a process to ensure that independent advice and comment on each plan developed in accordance with Section 6.b, above, is provided. Such advice and comment should be provided prior to developing a new system or significantly modifying an existing system.

d. Every agency must ensure that security plans incorporate appropriate internal control corrective actions identified pursuant to OMB Circular No. A-123.

e. Every agency must prepare materials as described in Section 8, meet with OMB, NIST, and NSA staff as described in Section 7, and work with NIST and NSA to improve agency computer security.

7. **Assistance Visits.**

a. Agencies will be scheduled for visits by OMB, NIST, and NSA staff. The purpose of these visits will be for OMB to discuss the agency's implementation of the Act. NIST and NSA will provide technical advice and assistance on the agency's security needs as requested.

b. Among the items to be discussed will be:

(1) The completeness of identification of sensitive computer systems;

(2) The quality, scope, and thoroughness of security plans;

(3) Any internal control weaknesses identified pursuant to OMB Circular No. A-123 related to computer systems, and plans for addressing those weaknesses;

(4) For agencies subject to OMB Bulletin No. 89-17, "Federal Information Systems and Technology Planning" their response to that Bulletin;

(5) Material available in accordance with Section 8, below.

c. Agencies should also be prepared to discuss the approach that is being taken to ensure that computer security plans for new or modified computer systems are prepared and reviewed.

8. **Material for Meetings.** Agencies should, at a minimum, have

the following information available:

a. agency-wide computer security policies and a summary of agency computer security procedures, standards, and requirements;

b. agency assignment of responsibilities for implementation and operation of the security program;

c. the agency management plan for ensuring implementation of system computer security plans that includes a description of:

   (1) the involvement of agency management,

   (2) how computer security plans are being integrated into information resources management plans,

   (3) the approach for ensuring that funds, personnel and equipment are planned for and budgeted, and

   (4) the implementation schedule;

d. the method used to identify the agency's sensitive systems;

e. any known agency needs for guidance or assistance.

9. **Information Contacts.** Questions regarding Appendix A and other specific plan preparation guidance should be addressed to Jon Arneson (301 975-3870). Questions concerning other aspects of this Bulletin may be directed to Ed Springer (202 395-4814.)

10. **Expiration.** This Bulletin will remain in effect until it is superseded by a revision to OMB Circular No. A-130 and incorporated into standards or guidelines to be issued by NIST.

Richard Darman

Richard G. Darman
Director

Attachment

OMB BULLETIN NO. 90-08
APPENDIX A

INSTRUCTIONS FOR PREPARING SYSTEM SECURITY PLANS

GENERAL

The objective of computer security planning is to improve protection of information and information processing resources. In order for plans for the protection of the resources to be adequate, the managers most directly affected by and interested in the information or processing capabilities must be comfortable that their information and/or processing capabilities are adequately protected from loss, misuse, unauthorized access or modification, unavailability, or undetected activities.

The purpose of the system security plan is to provide a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. The system security plan may also be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. Thus it should reflect input from various managers with responsibilities concerning the system, including functional "end users" or information owners, the system operator and the system security manager. Additional information may be included in the basic plan and the structure and format organized according to agency needs, so long as the elements described below are adequately covered and are readily identifiable.

It should be noted that plans for the security of contractor, State, and local systems that perform a Federal function may be significantly different from plans for Federally operated systems. The plans for such systems are Federal plans for actions intended to ensure against the risk of loss or harm from the Federal government's perspective. Thus, such plans might not require descriptions of specific developmental, operational, or technical controls as described in this Appendix, but of controls measured by functional performance criteria (e.g., limits on errors or requirements for certain levels of accuracy). The key in identifying such systems and planning for their security is to determine Federal risk and assess the best way to "insure" against that risk.

Each security plan for a Federally operated system should have four basic sections:

I System Identification

II Sensitivity of Information

III System Security Measures

IV Additional Comments

The remainder of this Appendix contains a description of the scope, content, and format of each of the four sections.

I. SYSTEM IDENTIFICATION

This section of the plan contains basic identifying information about the system.

A. **Responsible Organization** - The specific Federal organizational subcomponent responsible for the system being reported. If a State or local government or contractor is actually performing the function, identify both the Federal and other organization and describe the relationship.

B. **System Name/Title** - Logical boundaries must be drawn around the various processing, communications, storage, and related resources to define a system. For planning purposes, those systems in an agency or its subordinate elements under the same direct management control with essentially the same function, characteristics, and security needs may be treated as a single system. Each system name/title should be both meaningful and distinct from other system names/titles.

C. **System Category** - Categorize each system as either a major application, or as a general support system, in line with the primary management responsibility for the system.

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

- **General support system** - These consist of hardware and software that provide general ADP or network support for a variety of users and applications. Individual applications may be less easily distinguishable than in the previous category, but such applications may contain sensitive information. Even if none of the individual applications are sensitive, however, the support system itself may be considered sensitive if overall, the aggregate of applications and support provided are critical to the mission of the agency.

D. **System Operational Status** - One of the following:

- o Operational - system is currently in operation.

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

- o Undergoing a major modification - system is currently undergoing a major conversion or transition.

If the system is either under development or undergoing a major modification, provide information about methods being used to assure that up-front security requirements are included.

E. **General Description/Purpose** - A brief (1-3 paragraph) description of the function and purpose of the system (e.g., Medicare claims processing, network support for an organization, business census data analysis, crop reporting support, etc.).

Computer security requirements should be coordinated between end users and those responsible for any support system(s) being used. Plans for such requirements must be based on an understanding of what is being protected. Thus, if this is a general support system, the nature of the uses made or the applications being supported should also be described.

F. **System Environment and Special Considerations** - A brief (1-3 paragraphs) general description of the technical system. Include any environmental factors that cause special security concerns, such as: it is located in a harsh or overseas environment; software is rapidly implemented; it is an open network used by the general public or with overseas access; the application is processed at a facility outside of the agency's control; the general support mainframe has dial-up lines; etc.

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

II. SENSITIVITY OF INFORMATION HANDLED

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

A. **Applicable Laws or Regulations Affecting the System** - List any laws or regulations that establish specific requirements for confidentiality, integrity, or availability of information in the system. Examples might include the Privacy Act or a specific statute or regulation concerning the information processed (e.g., tax or census data). Note: This should not be a list of technical standards concerning how to protect systems once the need for such protection has been determined. For this reason, the Computer Security Act of 1987 should not be listed here.

If the system processes records subject to the Privacy Act, include the number and title of the Privacy Act system(s) of records and whether the system(s) is used for computer matching activities.

B. **General Description of Information Sensitivity** - The purpose of this section is to indicate the type and relative importance of protection needed for the identified system. A system may need protection for one or more of the following reasons:

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

o **Integrity** - The system contains information which must be protected from unauthorized, unanticipated or unintentional modification, including the detection of such activities. Examples: systems critical to safety or life support, financial transaction systems.

o **Availability** - The system contains information or provides services which must be available on a timely basis to meet mission requirements or to avoid substantial losses. Examples: air traffic control, economic indicators, or hurricane forecasting.

Describe, in general terms, the information handled by the system and the need for protective measures.

o Relate the information handled to each of the three basic protection requirements above (confidentiality, integrity, and availability).

o Include a statement of the estimated risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system. To the extent possible, describe this impact in terms of cost, inability to carry out mandated functions, timeliness, etc.

For each of the three categories (confidentiality, integrity, and availability), indicate if the protection requirement is:

o **High** - a critical concern of the system.

o **Medium** - an important concern, but not necessarily paramount in the organization's priorities.

o **Low** - some minimal level of security is required, but not to the same degree as the previous two categories.

III. SYSTEM SECURITY MEASURES

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

A. **Risk Assessment and Management** - Risk assessment and management are crucial elements of the security planning process which include identification of informational and other assets of the system, threats that could affect the Confidentiality / integrity / availability of the system, important system vulnerabilities to the threats, potential impacts from threat activity, identification of protection requirements to control the risks, and selection of appropriate security measures. How was the risk related to the above-listed factors determined for this system?

B. **Applicable Guidance** - Indicate, to the extent practical, specific standards or other guidance used in the design, implementation, or operation of the protective measures used on the system (e.g., relevant Federal or industry standards). This should include agency policy and guidance documents.

C. **Security Control Measures** - Two sets of controls are discussed on subsequent pages - one for Major Applications and the other for General Support Systems. Controls included should be addressed from the perspective of the individual having direct management responsibility for the system. For each system, only the set corresponding to the system category designated under Basic System Identification needs to be completed.

The controls described are derived from requirements and guidance in the Computer Security Act, OMB Circular No. A-130, Appendix III, "Management of Federal Information Resources," and applicable Federal Information Processing Standards and Special Publications produced by the National Institute of Standards and Technology.

D. **Security Control Measure Status** - For each control measure on the appropriate list, specify whether it is:

- In Place - Control measures of the type listed are in place and operational, and judged to be effective. Describe in general terms.

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

- <u>In Place and Planned</u> - Some measures are in place, while others are planned. A general description of the measures in place and those planned, including the resources involved and expected operational dates should be provided.

- <u>Not Applicable</u> - This type of control measure is not needed, cost-effective, or appropriate for this system. Explain.

NOTE. For operational systems, some specific controls of a given type may be "In Place," while others may be "Planned." For systems under development or undergoing a major modification, it is expected that many measures will be "Planned."

E. Security Control Measures for Major Applications

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

1. <u>MANAGEMENT CONTROLS</u> - overall management controls of the application system.

a. **Assignment of Security Responsibility** - Responsibility for the security of the application should be assigned.

b. **Personnel Screening** - Personnel security policies and procedures should be in place and working to limit access to and processing within the application system to those with a need for such access. Where appropriate, the duties of those with access should be separated. Additionally, requirements such as screening individuals with access to the application as well as those participating in the design, development, operation, or maintenance of it may be used.

2. <u>DEVELOPMENT/IMPLEMENTATION CONTROLS</u> - procedures to assure protection is built into the system, especially during system development.

a. **Security Specifications** - Appropriate technical, administrative, physical, and personnel security requirements should be specified for the application.

b. **Design Review and Testing** - A design review and systems test should have been performed for this application prior to placing it into operation, to assure the application meets the security specifications. The results of the design reviews and system tests should be fully documented and maintained in the official agency records.

c. **Certification** - Prior to the application being put into operation, an agency official should certify that the application meets all applicable Federal policies, regulations, and standards, and that protection measures appear adequate. If the application has been in operation for a period of time, it should have been audited or reviewed and recertified within the last three years.

3. OPERATIONAL CONTROLS - day-to-day procedures and mechanisms to protect operational application systems (or planned applications when they become operational).

a. **Physical & Environmental Protection** - Physical protections in the area where processing on the application system takes place (e.g., locks on terminals, physical barriers around the processing area, etc.).

b. **Production, I/O Controls** - Controls over the proper handling, processing, storage, and disposal of input and output data and media, as well as access controls (such as labeling and distribution procedures) on the data and media.

c. **Emergency, Backup, and Contingency Planning** - Workable procedures for continuing to perform essential functions in the event that information technology support is interrupted. They should be coordinated with the back-up and recovery plans of any installations/networks used by the application.

d. **Audit and Variance Detection** - Controls which allow management to conduct an independent review of records and activities to test the adequacy of controls, and to detect and react to departures from established policies, rules, and procedures. Variance detection for an application checks for anomalies in such things as the numbers and types of transactions, volume and dollar thresholds, and other deviations from standard activity profiles.

e. **Application Software Maintenance Controls** - Controls used to monitor the installation of and updates to application software to ensure that the software functions as expected and that an historical record is maintained of application system changes. Such controls also help to ensure that only authorized software is allowed on the system. These controls may include software configuration policy that grants managerial approval to modifications, then documents the changes. They may also include some products used for "virus" protection.

f. **Documentation** - Controls in the form of descriptions of the hardware, software, and policies, standards, and procedures related to computer security, to include backup and contingency activities. They also include descriptions of end user procedures. Documentation should be coordinated with the data center and/or network manager(s) to ensure that adequate application and installation documentation are maintained to provide continuity of operations.

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

a. **Security Awareness and Training Measures** - All employees involved with the management, use, design, development, maintenance or operation of the application should be aware of their security responsibilities and trained how to fulfill them.

5. TECHNICAL CONTROLS - hardware and software controls used to provide automated and/or facilitate manual protections. Normally these types of controls are coordinated with the network and/or data center manager.

a. **User Identification and Authentication** - Controls used to identify or verify the eligibility of a station, originator, or individual to access specific categories of information, to perform an activity, or to verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification. Such controls include the use of passwords, tokens, biometrics or other personal mechanisms to authenticate identity.

b. **Authorization/Access Controls** - Hardware or software features that are designed to permit only authorized access to or within the application, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists).

c. **Data Integrity/Validation Controls** - Controls used to protect data from accidental or malicious alteration or destruction, and provide assurance to the user that the data meets an expectation about its quality (e.g., EFT message authentication). Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirements.

d. **Audit Trails and Journaling** - Controls that provide a transaction monitoring capability with a chronological record of application activities. This enables reconstruction of a transaction from its inception to final results -- including any modification of files.

6. COMPLEMENTARY CONTROLS PROVIDED BY SUPPORT SYSTEMS - The person responsible for the application should understand and

accept the risk inherent in processing on the network or at the installation(s) that support the application, particularly where the support system is operated outside of their management control (e.g. by another agency). If not, plans for greater understanding of that risk should be described.

F. **Security Control Measures for General Support Systems**

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

1. MANAGEMENT CONTROLS - overall management controls of the general support system.

a. **Assignment of Security Responsibility** - Responsibility for the security of each support system should be assigned to a management official knowledgeable in information technology and security matters.

b. **Risk analysis** - A risk analysis consists of a structured approach to identify assets, determine threats and vulnerabilities, estimate potential impacts, identify applicable controls and their costs, and select cost-effective controls for use. Include the name of any automated or formalized manual methodology used.

c. **Personnel Screening** - Personnel security policies and procedures should be in place and working to control access to and within the support system to assure that only those with a need for access have it. Such policies and procedures may include requirements for screening individuals involved in the operation, management, security, design, programming, or maintenance of the system.

2. ACQUISITION/DEVELOPMENT/INSTALLATION CONTROLS - procedures to assure that protection is built into the system.

a. Acquisition Specifications - Appropriate technical, administrative, physical, and personnel security requirements are to be included in specifications for the acquisition or operation of information technology installations, equipment, software, and related services.

b. Accreditation/Certification - Accreditation is management authorization and approval to process sensitive information in an operational environment. Issued by a designated official, it usually includes any constraints for processing in the environment. It is normally based on a certification, which is a technical evaluation that indicates how well a design/implementation meets a specified set of computer security requirements.

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

a. **Physical & Environmental Protection** - Controls used to protect against a wide variety of physical and environmental threats and hazards including deliberate intrusions, natural or man-made hazards, and utility outages or breakdowns (e.g., computer room locks, special fire fighting equipment, "hardened" communications, etc.).

b. **Production, I/O Controls** - Controls over the handling, processing, storage, and disposal of input and output from the support system (e.g., controlled or locked output boxes, tape or data screening, etc.).

c. **Emergency, Backup, and Contingency Planning** - Appropriate emergency, backup and contingency plans should be in place and tested regularly to assure the continuity of support in the event of system failure. These plans should be known to users and coordinated with their plans.

d. **Audit and Variance Detection** - Controls that allow management to conduct an independent review of system records and activities in order to test for adequacy of system controls, and to detect and react to departures from established policies, rules, and procedures. Variance detection includes the use of system logs and audit trails to check for anomalies in the number of system accesses, types of accesses, or files accessed by users.

e. **Hardware and System Software Maintenance Controls** - Controls used to monitor the installation of and updates to hardware and operating system and other system software to ensure that the software functions as expected and that an historical record is maintained of system changes. They may also be used to ensure that only authorized software is allowed on the system. These controls may include hardware and system software configuration policy that grants managerial approval to modifications, then documents the changes. They may also include some products useful for "virus" protection.

f. **Documentation** - Controls in the form of descriptions of the hardware, software, and policies, standards, and procedures related to computer security on the support system, to include backup and contingency activities. They also include descriptions of operator procedures.

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

a. **Security Awareness and Training Measures** - All employees who are involved with the management, use, design, acquisition, maintenance or operation of the support system should be aware of their security responsibilities and trained how to fulfill them.

5. TECHNICAL CONTROLS - hardware and software controls to protect the general support system from unauthorized access or misuse, to facilitate detection of security violations, and to support security requirements for associated applications.

a. **User Identification and Authentication** - Controls used to verify the identity of a station, originator, or individual prior to allowing access to the system, or specific categories of information within the system. Such controls may also be used to verify that only authorized persons are performing certain processing activities on the system. These controls include the use of passwords, tokens, or biometrics or other personal mechanism to authenticate an identity.

b. **Authorization/Access Controls** - Hardware or software features used to detect and/or permit only authorized access to or within the system (e.g., the use of access lists). Includes controls to restrict access to the operating system, limits on access to programming resources, and controls to support security policies of associated applications.

c. **Integrity Controls** - Controls used to protect the operating system, applications and information in the system from accidental or malicious alteration or destruction, and provide assurance to users that data has not been altered (e.g., Message authentication). Note. Operating system controls and system administration procedures, which are normally described in vendor supplied documentation, should be followed.

d. **Audit Trail Mechanisms** - Controls that provide a system monitoring and recording capability to retain a chronological record of system activities. Such controls normally enable the reconstruction of system activity. The use of system log files is an example of this type of control.

e. **Confidentiality Controls** - These controls provide protection for data that must be held in confidence and protected from unauthorized disclosure. The controls may provide data protection at the user site, at a computer facility, in transit, or some combination of these (e.g., encryption).

6. CONTROLS OVER THE SECURITY OF APPLICATIONS - The security of each application that processes on a support system affects the security of all others processing there. Thus the manager of the support system should understand the risk that each application represents to the system. If not, plans for greater understanding of that risk should be described. (e.g., Application users that have access to programming capability represent a higher risk to the support system than when they are confined to individual application functions. Similarly, applications that utilize dial-up communications represent a higher risk.)

IV. ADDITIONAL COMMENTS

This final section is intended to provide an opportunity to include additional comments about the security of the subject system and any perceived need for guidance or standards.

NUREG/BR-0166

INSTRUCTIONS FOR PREPARING SECURITY PLANS FOR LOCAL AREA NETWORKS IN COMPLIANCE WITH OMB BULLETIN NO. 90-08

FEBRUARY 1992