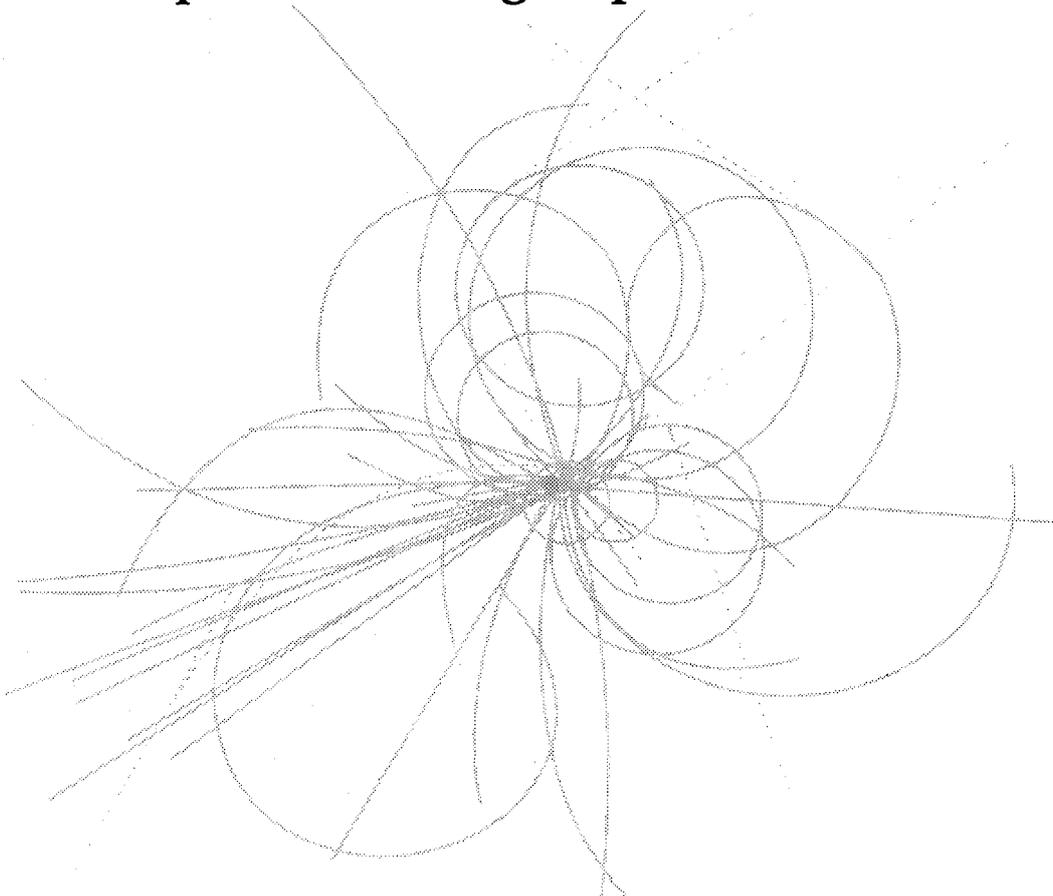


Superconducting Super Collider Laboratory



Computer Protection Plan for the Superconducting Super Collider Laboratory

April 1992

**Computer Protection Plan
for the Superconducting
Super Collider Laboratory**

Superconducting Super Collider Laboratory*
2550 Beckleymeade Ave.
Dallas, TX 75237

April 1992

*Operated by the Universities Research Association, Inc., for the U.S. Department of Energy under Contract No. DE-AC35-89ER40486.

COMPUTER PROTECTION PLAN
FOR THE
SUPERCONDUCTING SUPER COLLIDER LABORATORY

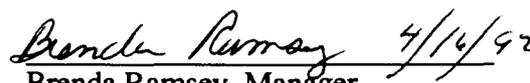
April 15, 1992

Prepared by : Sharon Hunter, ACPPM

Approved by:


Bob Hahn, CPPM
Information Services/GMO

Reviewed by:


Brenda Ramsey, Manager
Computer Operations
Information Services/GMO

Approved by:


Dee Lersch, Manager
Information Services/GMO
Senior ADP Officer

TABLE OF CONTENTS

TABLE OF CONTENTS.....	ii
1.0 PURPOSE AND SCOPE	1
1.1 References.....	1
2.0 COMPUTER PROTECTION PERSONNEL.....	2
2.1 Computer Protection Program Managers and Assistants	2
2.2 Security Incident Response Personnel.....	2
2.3 Emergency Response Personnel.....	2
3.0 EMERGENCY NOTIFICATION PROCEDURES.....	3
3.1 Disaster Emergency Notification Procedures	3
3.2 Computer Security Incident Reporting Procedure.....	3
3.3 Actions Taken for Computer Security Incidents and Violations	3
4.0 MANAGEMENT CONTROL PROCESS	6
4.1 Management Control Procedures.....	8
4.1.1 Periodic Risk Assessments	8
4.1.2 Functional Security Requirements and Specifications	8
4.1.3 Security Design Reviews and System Tests	9
4.1.4 Certification of Systems and Sensitive Applications.....	9
4.1.4.1 Annual Use Certification Criteria	10
4.1.5 Security Specifications for Acquisitions.....	11
4.1.6 Compliance Review Follow-up Procedures	11
4.2 Administrative Safeguards	11
4.2.1 Reviewing Computer Files at Random	11
4.2.3 System Access.....	11
4.3 Technical Controls	12
4.4 Physical Controls.....	14
4.4.1 Controlled Entrances/Exits.....	14
4.4.2 Locks	14
4.5 Personnel Safeguards.....	14
4.5.1 Screening of Non-Federal Personnel	14
4.5.2 Personal Accountability of Sensitive Information.....	14

4.5.3	Users Knowledge of Responsibilities, Policies & Procedures	14
5.0	SYSTEM IDENTIFICATION.....	15
5.1	Computer Systems Hardware Identification	15
5.1.1	Overview Sensitive/Unclassified Systems	15
5.1.2	Mission-Essential/Unclassified Systems	15
5.1.3	Critical Systems	15
5.1.4	Unclassified Communications Systems	15
5.2	Computer Systems Software Identification	16
5.2.1	Sensitive/Unclassified Applications.....	16
5.2.2	Mission-Essential/Unclassified Applications	16
5.2.3	Critical Applications	16
5.2.4	Software Security Tools.....	16
6.0	PLANS	17
6.1	Security Awareness and Training Plan	17
6.2	Contingency Plan.....	17
6.2.1	Operational Tests.....	19
6.2.2	Formal Written Agreement.....	19
6.3	Disaster Recovery Plan	19
7.0	SCHEDULES	19
7.1	Risk Assessments and Management	19
7.2	Certification and Re-certification	20
7.3	Security Awareness and Training Sessions	20
8.0	REVIEWS.....	20
8.1	Compliance Review Results and Recommendations.....	20
8.2	Security Design Reviews.....	20
8.3	System Tests.....	20
8.4	Risk Assessments	20
	APPENDIX A.....	22
	APPENDIX B.....	25
	APPENDIX C.....	27
	APPENDIX D.....	29
	Attachment 1	33
	Attachment 2	54

1.0 PURPOSE AND SCOPE

The purpose of this document is to describe the current unclassified computer security program practices, policies and procedures for the Superconducting Super Collider Laboratory (SSCL). This document includes or references all related policies and procedures currently implemented throughout the SSCL. The document includes security practices which are planned when the facility is fully operational. A glossary of terms used in this document is included in Appendix A.

This document is prepared and maintained by the Computer Protection Program Manager (CPPM) for use by management and computer security contacts. It is prepared in accordance with the Department of Energy (DOE) Order 1360.2A regarding Unclassified Computer Security. This document is reviewed annually by the CPPM and updated as necessary.

1.1 References

The SSCL policies are contained in the Management Plan for Computing Services. Specific policies relating to the Unclassified Computer Security Program include:

COMPUTER PROTECTION PROGRAM PRACTICE (MAY 1991, T10-0000009, REV A)

COMPUTER SECURITY AWARENESS AND TRAINING GUIDELINE (DOE, FEB. 1988)

COMPUTER SECURITY AND PRIVACY PLAN (REVISED 6/26/91)

DISASTER RECOVERY PROGRAM GUIDELINE (DOE, JULY 1991)

DOE ORDER 1360.1A, ACQUISITION AND MANAGEMENT OF COMPUTING RESOURCES

DOE ORDER 1360.2A, COMPUTER SECURITY PROGRAM FOR UNCLASSIFIED COMPUTER SYSTEMS

EMERGENCY PREPAREDNESS PLAN

SECURITY GUIDELINES FOR UNCLASSIFIED MICROCOMPUTER USERS, MAY 1990.

SSCL LABORATORY COMPUTER OPERATIONS MANUAL, COMPUTER OPERATIONS, GROUP, SEPT.1991

SSCL LABORATORY POLICY, COMPUTER OPERATIONS POLICY (MAY 1991, T10-0000001, REV B)

SSCL POLICY FOR COMPUTING AND COMMUNICATION (JAN. 1991) 01.A

2.0 COMPUTER PROTECTION PERSONNEL

2.1 Computer Protection Program Managers and Assistants

The unclassified computer security program for the SSCL is organized under the direction of the CPPM. The function of the CPPM falls under the direction of Information Services within the SSCL. It is the intent of the SSCL to require all personnel appointed in the unclassified computer security program to have demonstrated knowledge and background in computer science, as well as to have a clear understanding of computer security practices and techniques.

To assist in administering the computer security program, computer security contacts will be appointed by their Associate Director (AD) and will be responsible for specific systems and locations. As each Assistant Computer Protection Program Manager (ACPPM) is appointed, written notification is to be sent to the CPPM for approval.

2.2 Security Incident Response Personnel

Personnel responsible for responding to unclassified computer security incidents include the CPPM, ACPPM and computer security contacts. It is the responsibility of the CPPM and division computer security contacts to assess and document potential computer security incidents and report them immediately to upper management. Under the direction of CPPM, the computer security contacts are responsible for responding to all other security matters including incidents involving government property. The CPPM will contact the appropriate ACPPM in accordance with the Guidelines set forth in the DOE Order 1360.2A.

2.3 Emergency Response Personnel

The Emergency Response Personnel for noncomputer related issues are covered in the Emergency Preparedness Plan (EPP). The Emergency Preparedness Plan includes lists of the teams from Building Maintenance, Building Services, Fire Protection Services, Safety and other personnel. The EPP listings include areas of responsibility, names, and phone numbers of team leaders responsible for each of the areas. To support the EPP an additional Emergency Contact Team is designated for each of the SSCL sites.

The Emergency Response Personnel for computer related emergencies are identified and outlined in the Risk Assessment and Contingency Plan Document for each SSCL site. The Emergency Response Personnel list is maintained by each of the designated groups per site. The lists are maintained, distributed, and updated by the Emergency Response Team leaders. The Emergency Response Personnel list is kept on file with the CPPM, ACPPM and Contingency Plan for each site. Appendix B outlines the areas covered for each of the Site Emergency Response teams.

3.0 EMERGENCY NOTIFICATION PROCEDURES

Procedures for emergencies classified as a computer security incident emergency or a disaster emergency are described. A computer security incident will involve the CPPM for evaluation and handling. Whereas, a disaster emergency will be evaluated and handled by the Emergency Preparedness manager in accordance with the Emergency Preparedness Plan. The following sections describe the procedures to be followed depending upon the type of emergency involved.

3.1 Disaster Emergency Notification Procedures

Procedures for following disaster notification are provided in the Emergency Preparedness Plan (EPP). If a computer related emergency occurs, the Computer Operations Manager along with the appropriate Emergency Response Teams listed in Section 22 of the Emergency Preparedness Plan are notified. The CPPM, along with other designated personnel, and Computer Operations Manager will determine the appropriate response, taking into account the procedures specified in the Contingency Plan document. The Emergency Preparedness Plan manager shall request assistance in coordinating with other inside or outside organizations as necessary.

If the CPPM is not available, the ACCPM or other management personnel should then notify the Manager of Information Services.

3.2 Computer Security Incident Reporting Procedure

The procedure for reporting computer security incidents is outlined in DOE Order 1360.2A, see Attachment 1. Computer security contacts will follow that procedure for reporting computer security incidents to the CPPM. The CPPM will then determine the significance of the incident. If it is determined to be a reportable, significant incident according to Guidelines set forth in DOE Order 1360.2A, the CPPM notifies the Computer Protection Program Coordinator (CPPC) at the DOE/SSCPO and appropriate managers. The CPPM follows the procedures shown in Figure 3-1 for reporting a significant computer security incident.

The CPPM retains documentation on all reported and suspected incidents. The CPPM supplies information similar to that listed in DOE Order 1360.2A for identifying and reporting a significant incident, such as a general description of what has happened, who is thought to be involved, and what corrective action has been taken or is planned. An example of the follow-on report format used in documenting computer security incidents is displayed in Figure 3-2.

3.3 Actions Taken for Computer Security Incidents and Violations

Actions constituting suspected or confirmed significant computer security incidents are brought to the immediate attention of the CPPM as described in Section 3.2. Reasonable steps are taken to minimize the probability of further occurrence including counseling, disciplinary actions, and/or notifying criminal investigative and law enforcement authorities, as appropriate.

Computer Security Incident Reporting Procedures

(Process followed by CPPM)

Report Incidents to Manager of Information Services

Determine action to be taken

Inform DOE/SSCPO other sites might be affected

Review computer security incidents with personnel involved

Implement corrective actions to be taken

Maintain a file of computer incident reports

Figure 3-1

Follow-on Security Report

Date: **Report Type:** Unclassified
Time of Incident: **Report Number:**
Location of Incident: **Division/Organization**
CPPM Name: **Phone:**
Hardware System:
Operating System:
Description:
Effects of Incident:
Action Taken:
Contacts Notified:
Implication for Other Sites:
Recommendations:
Resolutions: **Comments:**

Figure 3-2

4.0 MANAGEMENT CONTROL PROCESS

In accordance with DOE Order 1360.2A, the SSCL has established the unclassified computer security program to appropriately:

- a. Protect DOE unclassified computer systems from abuse and misuse.
- b. Protect sensitive-unclassified automated information from unauthorized access, alteration, disclosure, destruction, or improper use as a result of improper actions or adverse events.
- c. Prepare contingency and disaster recovery plans to provide reasonable continuity of operations for unclassified computers, and in particular, DOE mission-essential applications/functions.
- d. Use physical, personnel, administrative, hardware, and software security measures to protect systems and information based on results of risk assessments.

Criteria set forth by CPPM and Information Services ensures protection of sensitive applications. All sensitive applications are documented by the user, database administrator, developer, IS manager and Computer Operations manager. Documentation includes service requests, program documentation and sensitivity questionnaire forms. The management control process, as illustrated in Figure 4-1 on the next page, ensures that the sensitivity and/or essentiality of the information processed on a computer is determined by the owners of the information. Appropriate protection measures should be taken. Procedures are incorporated into all new and operational unclassified computer systems/applications processing sensitive information to achieve and sustain an acceptable level of security.

Unclassified Computer Security Program Management Controls

Every Year

**Annual Use Certifications
Sensitivity Questionnaires
Microcomputer Security Agreements**

Every 2 Years

Site Security Level Questionnaires

Every 3 Years

**Risk Assessment/Contingency Plans
Sensitivity Review of Applications
DOE Appraisals**

Figure 4-1

The unclassified computer security program includes procedures for conducting periodic risk assessments, defining functional security requirements and specifications, conducting security design reviews and system tests, certifying and re-certifying sensitive applications, and approving security specifications for acquisitions. Follow-up procedures include ensuring implementation of recommendations from compliance review activities. These procedures are described in the following sections.

4.1 Management Control Procedures

4.1.1 Periodic Risk Assessments

Periodic risk assessments are conducted in accordance with the practices described in the document SSCL Practice, Computer Protection Program Practice, May 1991, T10-000009, Rev. A. The aim of the assessments is to ensure that appropriate, cost effective safeguards are incorporated with the associated computer systems and unclassified information processed.

Risk assessments are performed prior to construction or operational use of a new computer installation, whenever there is a significant change to the existing computer installation, and at periodic time intervals not to exceed 5 years. These risk assessments, along with contingency plans, are reviewed and approved by the CPPM. The CPPM retains a log of all completed risk assessments. Written correspondence documents action taken or planned as a result of the risk assessment findings and recommendations.

Risk assessments are performed at the computer installation where the computer applications will be processed. The results of the risk assessments are taken into consideration when defining and approving security specifications for computer applications. Risk assessment documents which identify either existing protective measures, or a vulnerability are treated as sensitive unclassified information. They are maintained in locked files for protection.

4.1.2 Functional Security Requirements and Specifications

SSCL IS is responsible for development of all administrative type applications, therefore controlling all major sensitive-unclassified administrative systems. Definitions of the Functional Security Requirements and Specifications are outlined in the document SSCL Practice, Computer Protection Program Practice, May, 1991, NO.T10-000009, Rev. A.

Function security requirements are defined by information owners based on the sensitivity of information to be processed, and how the application or information may be vulnerable. The potential impact is assessed if sensitive information is misused, altered, destroyed or disclosed.

Specifications developed by SSCL IS describe how specific protective techniques are employed. Specifications are described in technical terms that programmers and system developers can implement. Specifications are contained in a policy statement issued by the IS manager regarding all application system development .

Functional security requirements and security specifications are reviewed and approved prior to acquiring or starting formal development. For applications to be developed, approval signatures are documented on Information Service Project Request forms and Production Change Control

forms. Functional security requirements and specifications for hardware are reviewed and approved at the time of requisitioning see Section 4.1.5 for a description of the process.

4.1.3 Security Design Reviews and System Tests

Security design reviews and system tests are conducted and approved in accordance with the practices listed in the document SSCL Practice, Computer Protection Program Practice, May 1991, T10-000009, Rev. A.

Security design reviews and system tests are conducted and approved prior to operational use of unclassified computer applications. Reviews are conducted by the programming area with the appropriate representatives from the user organizations. Security measures are reviewed and approved by the CPPM.

Upon successful completion of testing, the unclassified computer application is certified by the CPPM. The CPPM determines that the applications and operational procedures meet the security requirements and are adequately protected. Certification for Administration applications is documented on the original Information Services Project Request and Production Change Control forms.

4.1.4 Certification of Systems and Sensitive Applications

Overall system certification is accomplished by annual review of each system by the CPPM to determine which applications, if any, are considered sensitive, critical or mission-essential. Results of this review are documented on the Annual Use Certification and Sensitivity Questionnaire forms as requested by the CPPM. The Annual Use Certifications are signed and returned to the CPPM. The Sensitivity Questionnaires remain with the division computer security contacts. The Annual Use Certification criteria is summarized in Figure 4-2 on the next page.

In addition to annual system certification, sensitive applications are reviewed every three years to determine level of sensitivity and ensure that adequate protection measures are being implemented. The review is held by the CPPM and coordinated with the internal auditor and/or appropriate members of the user organization. Results of these reviews are documented and maintained on file with the CPPM and/or internal auditor. The re-certification process takes into consideration all available information, including other prior reviews and audits conducted. If no significant change has taken place and no deficiencies have been indicated in other review activities, the re-certification process may be less stringent than the initial certification process.

4.1.4.1 ANNUAL USE CERTIFICATION CRITERIA

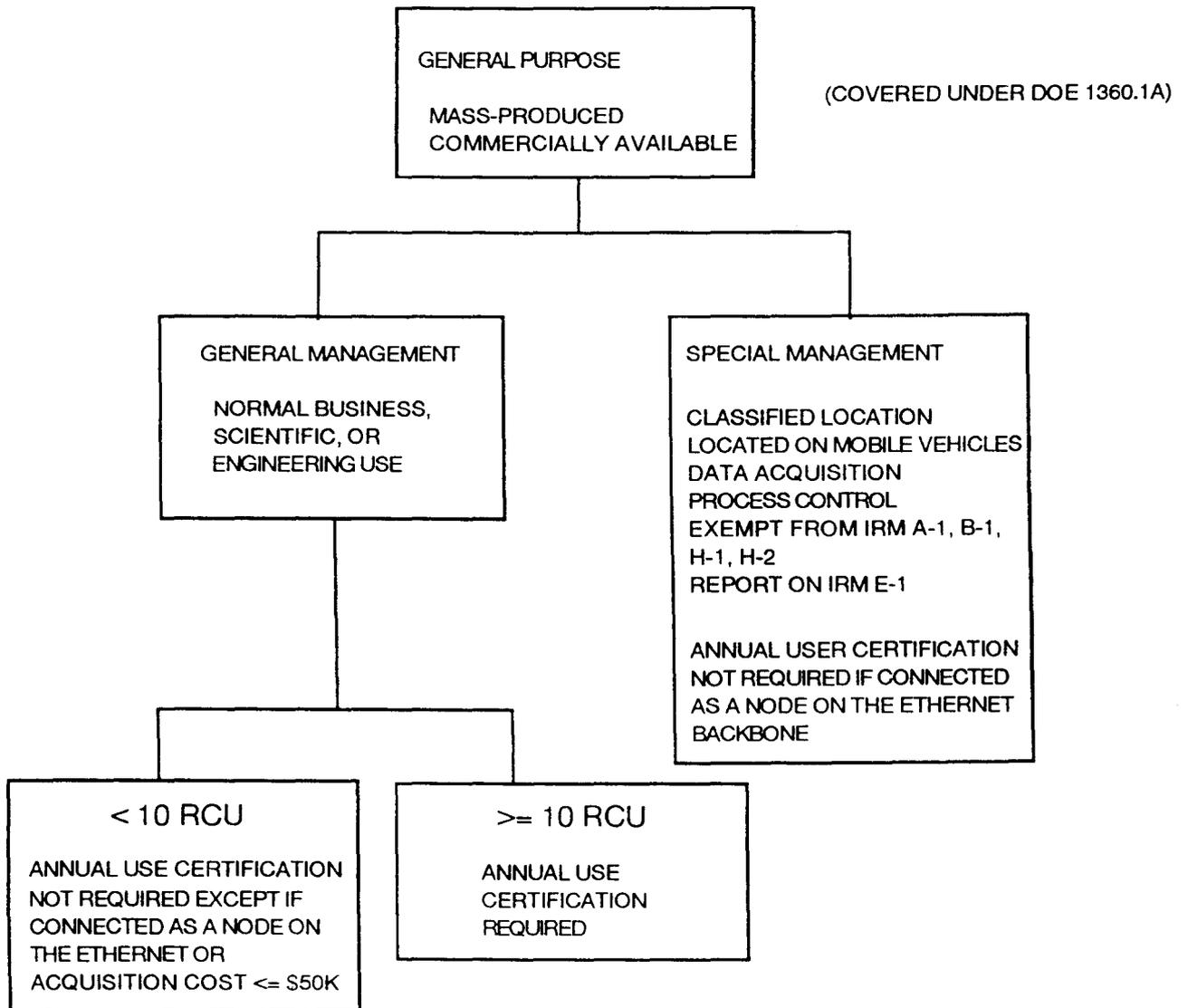


FIGURE 4-2

4.1.5 Security Specifications for Acquisitions

All computer system acquisition plans for computing resources and communications hardware and software are reviewed and approved by the CPPM. The plans are then submitted to the DOE/SSCPO. The Statement of Strategy, Acquisition Plan and Implementation Plan all address security and are approved by the CPPM prior to acquisition.

For the acquisition of equipment and software, or related services, appropriate functional security requirements are incorporated into the acquisition documents. Functional security requirements are reviewed and approved by the CPPM prior to acquisition, to ensure that they are reasonably sufficient for the intended application, and that they comply with current computer security policies, procedures, and standards. If users have not devised appropriate, adequate security measures, the CPPM withholds approval until the requirements for security have been met.

4.1.6 Compliance Review Follow-up Procedures

Correspondence is maintained with DOE/SSCPO regarding all findings and recommendations resulting from a Compliance Review until all items are resolved and closed.

4.2 Administrative Safeguards

4.2.1 Reviewing Computer Files at Random

The software for randomly selecting computer files for review is available. The number of files and time interval for reviews is determined by the Computer Operations Manager or appropriate Systems Manager. Different criteria are used depending on the size and sensitivity level of the systems. For the majority of systems, an automated program exists which can randomly select files to be reviewed, print the first few lines of the file, and produce a listing.

4.2.3 System Access

Users are required to initiate a Computer Account Request Form for system access and submit it to the appropriate authority for approval. All requests for an account on the central computing resources must have the approval of the Section, Group or Department Manager for each user. Completed User Validation Request Forms are kept indefinitely in the Computer Operations vaults.

Passwords are issued in a protected fashion. Temporary passwords are assigned to each user by the computer security contacts for that system. Passwords on all VAX/VMS accounts are set to expire every 180 days. Password expiration will be implemented for systems using mission-essential and critical application. Passwords given verbally for any system must be changed immediately upon system access. Users are responsible for protecting their passwords.

4.3 Technical Controls

Procedures have been established using controls designed to prevent and/or detect misuse and abuse of unclassified computer resources. Automated computer systems logs of accesses are maintained for multi-user computer systems to determine whether unauthorized accesses are being used. Various technical controls used to protect the unclassified computer resources include the following: Password Controls, Audit Trails, Record of Log-Ins, Sensitive Applications Special Controls, Keystroke Capturing and Random File Audits on major systems. (See Figure 4-3.)

A security access id card is being implemented on the Administrative Systems which process unclassified sensitive data. The cards provides a means of positively identifying users before they gain access to the Computers. The security card improves access security and eliminates problems of password abuse and electronic evesdropping. The security access provides a complete audit trail, produces an alarm, prevents passwords from being loaned, cannot be copied, detects hacking and tampering, and defeats observation from electronic evesdropping.

**UNCLASSIFIED COMPUTER SECURITY PROGRAM
TECHNICAL CONTROLS**

**Security ID Card Access Control
Password Controls**

Audit Trails

Record of Logins

Frequent Backups

Off-site Backups

Sensitive Applications Special Controls

Log File Audits

Figure 4-3

4.4 Physical Controls

4.4.1 Controlled Entrances/Exits

A Facility Security Plan has been prepared by the SSCL Security Section in accordance with the DOE/CH Safeguards and Security Division. These plans are the practice of the SSCL Security Section. Entrances and exits to all SSCL facilities are protected by locked door and access restricted as defined in the Facility Security Plan. Either key, electronic card or electronic combination locks are used. During building rounds, security performs site checks to computer areas.

4.4.2 Locks

Access to computer rooms and server rooms are controlled by electronic locks, card access and/or logs. Keys and/or combinations are changed as appropriate when key personnel no longer require access. Computer room access is controlled by the Applications Support Manager. An electronic card is used for access to the Computer Room.

4.5 Personnel Safeguards

4.5.1 Screening of Non-Federal Personnel

Employees who participate in managing, designing, developing, operating, or maintaining unclassified computer applications processing sensitive information, or who access automated sensitive unclassified information, are screened through the pre-employment background investigation. The Personnel Department conducts the screening process. The process includes personal reference checks, verification of past employment, and verification of education.

4.5.2 Personal Accountability of Sensitive Information

Appropriate protection measures are established for maintaining personal accountability for users granted access to sensitive unclassified data. Access is limited to no more information than authorized. Access control security cards, special application controls, passwords and audit trails are used to protect sensitive unclassified automated information.

Access to sensitive unclassified data on is granted by the System Managers upon receipt of the proper Data Request Form. The form must be signed by the SSCL Manager responsible for the integrity of that data. Authorization from the owners of the data is required before access to sensitive data is granted. The System Manager signs the form and maintains the original with the Computer Operations records. Users requiring access to sensitive information must have completed a Computer Account Request Form as described in Section 4.2.3.

4.5.3 Users Knowledge of Responsibilities, Policies & Procedures

All personnel who access unclassified computer systems are required to have a working knowledge of unclassified computer security responsibilities, policies, procedures, and administrative or legal actions. Employees and supervisors are responsible for reviewing SSCL

guidelines and documentation on computer security practices provided by the Information Services. Direction is also provided through the "Security Guidelines for Unclassified Microcomputer Users" document as well as in the Computer User's Guide. Personnel who process unclassified sensitive data are responsible for protecting that data in compliance with the DOE Order 1360.2A.

5.0 SYSTEM IDENTIFICATION

5.1 Computer Systems Hardware Identification

The overall computing environment at the SSCL is highly distributed, but with a significant centrally operated service facility. All multi-user systems are networked together, and access is provided to any systems from any terminal through the telecommunications network. The central computing facility provides VAX/VMS and UNIX services. In addition, there are numerous workstations, minicomputers and special-purpose processors. See Attachment 2 for a schematic of the current hardware configuration. A full description of hardware is covered in Part 3, "Computing Resources," of the Information Resources Management (IRM) Plan submitted to DOE/CH annually.

5.1.1 Overview Sensitive/Unclassified Systems

The CPPM retains a list of all computing resources of the SSCL based on the existing Property Management System. Sensitive/Unclassified computing resources of the SSCL supports a multi-vendor environment. The distributed environment consists of a network configuration of VAX clusters and UNIX servers linked with various Macintoshes, IBM, IBM/PC compatibles and UNIX workstations.

Within the computer configuration at the SSCL, there are two VAX/VMS systems which process sensitive data. The SSCAD1 VAX and SSCAD2 VAX, referred to as the Administrative Systems, process sensitive data. The SSCAD1 is a VAX 6420 with 128 MB of memory. The SSCAD2 is a VAX 6640 with 512 MB of memory. See Attachment 2 for a hardware schematic of the SSC Distributed Systems.

5.1.2 Mission-Essential/Unclassified Systems

The CPPM is responsible for retaining the list of all Mission-Essential/Unclassified systems. This list would be compiled from information supplied by each division on the Annual Use Certification form.

5.1.3 Critical Systems

The CPPM is responsible for retaining the list of all Critical systems. This list would be compiled from information supplied by each division on the Annual Use Certification form.

5.1.4 Unclassified Communications Systems

The unclassified communications networks are identified in Part IV, "Telecommunications," of the Information Resource Management (IRM) Plan submitted to DOE/CH annually. The SSCL General Data Network is a multi-vendor, multi-media system. It is designed to support a wide

variety of protocols and provide connectivity among remote SSCL sites. The SSCL sites connect to other DOE installations, as well as to universities and project subcontractors. There are three major locations described in the (IRM) Plan. External and internal security is addressed in the General Data Network configuration. External controls include dialup connections to a server with limited access. All security security requirements are coordinated between the CPPM and the telecommunications manager.

5.2 Computer Systems Software Identification

5.2.1 Sensitive/Unclassified Applications

The CPPM retains a list of all Sensitive/Unclassified applications. This list was reported to DOE in accordance with Public Law 100-235. This list is compiled from information supplied on the Annual Use Certification form by CPPM.

5.2.2 Mission-Essential/Unclassified Applications

The CPPM is responsible for retaining the list of all Mission-Essential/Unclassified application systems. This list will be compiled from information supplied by each division on the Annual Use Certification form.

5.2.3 Critical Applications

The CPPM is retains a list of all Critical applications. This list will be compiled from information supplied by each division on the Annual Use Certification form.

5.2.4 Software Security Tools

In general, the unclassified computer security program condones using security mechanisms supplied with the operating system and/or hardware by the vendor as appropriate. Additional security tools are continually being investigated by the CPPM and ACPPM. Software security tools are installed on microcomputers where sensitive data is predominantly processed. In the distributed environment, every effort is made to provide copies of the software tools necessary to protect data. File auditing, input keystroke auditing, controlled systems access are tools used to guard the data.

6.0 PLANS

6.1 Security Awareness and Training Plan

Security awareness and training is provided through off-site and on-site classes, memorandums, posters and lectures. New hire employees are receive a memorandum regarding security policy during orientation. Direction is provided through the "Security Guidelines for Unclassified Microcomputer Users" provided to all employees. The CPPM retains a signed security statement for employees. Updated information regarding policy or procedure changes is sent through internal memorandums and electronic mail. The distribution of the Computer Incident Advisory Capability (CIAC) Information Bulletins provide one method of increasing security awareness throughout the SSCL. The Usenet bulletin board is used as a means of communicating security issues. The techniques used in the Computer Security Awareness Training are summarized in Figure 6-1.

6.2 Contingency Plan

The purpose of the Contingency Plan is to provide action in the event of emergency conditions which would prevent the SSCL from meeting contractual obligations. The scope of contingency plan applies to mission-essential, critical or sensitive applications operated on SSCL computing systems where the consequences of the condition would result in the loss of assets, unauthorized disclosure of sensitive or personal data, or inability to restore critical programs, including system software and files.

All data on the Administrative Systems is backed up daily, weekly, and monthly. A list of the systems backup is retained for one month. Incremental backup procedures are followed daily. An image backup is performed weekly. Administrative production data directories are backed up nightly and copied to optical disks and tape daily. Month-end and year-end data are store indefinitely.

An Alternate Site Plan for the Administrative Systems and Scientific VAXes outlines the procedure to be followed in the event that the systems are rendered inaccessible beyond the deadline for critical purposes. A formal written agreement has been incorporated with Digital Equipment Corporation (DEC) to provide back-up services for outages lasting more than three to five days. The Computer Operations Manager will determine the criticality and contact appropriate personnel as necessary.

Contingency Plans are prepared every three years, or when a significant change occurs in location, hardware, applications or computer security contacts. The plans are combined with the Disaster Recovery Plan. Operational tests of the Contingency Plan include coordinating testing for the off-site backup of critical data. The Computer Operations Manager controls the tests of the Contingency Plan for the Administrative Systems in Computer Operations.

Computer Security Awareness Training

- **Security Guidelines**

 - Signed acknowledgement returned to CPPM

- **Classroom Training**

 - Guidelines used in classroom

 - Security film

 - Security training in new employee orientation

- **Security Memorandums**

 - Message outlining user responsibility

Figure 6-1

6.2.1 Operational Tests

Operational tests for contingency planning purposes are in the planning stage. It is the responsibility of Information Services, to plan, schedule, and coordinate off-site operational testing for the essential computer equipment. Since most hardware, operating systems, and product software is homogeneous, and no critical applications exist at the other SSCL sites, backup testing of each individual site is not required.

6.2.2 Formal Written Agreement

A formal written agreement exists between the SSCL and Digital Equipment Corporation for the scientific (SSCVX1) and the administrative (SSCAD1 & SSCAD2) computers. Off-site emergency back-up processing of critical applications are provided for in this agreement. DEC's Recover-all Service will aid in establishing a rapid and orderly response to a disaster situation. A formal written agreement is not necessary for arrangements made within SSCL for emergency backup services.

6.3 Disaster Recovery Plan

The Disaster Recovery Plan (DRP) for the SSCL describes program administrative procedures, continuity of operations plans, contingency plan disaster recovery plan management of policy and procedures, situation assessment, response selection process, post-disaster management and post disaster review and evaluation. The Risk Assessment and Contingency Plan document contains supplemental information to the DRP.

The DRP outlines the personnel, equipment and software needed for restructuring the SSCL computing environment. The method to notify personnel, implement a new alternate location, adapt to the new environment and evacuation procedures are described in the alternate site plan. In cases where outages extend beyond the limits specified, appropriate area supervisors are contacted and the decision to implement the alternate site plan is determined.

7.1 Risk Assessments and Management

The Los Alamos Vulnerability Assessment (LAVA) kit, which was developed by the DOE Center for Computer Security, was used to initially conduct a qualitative risk assessment. Additional risk assessments are performed prior to operation of a new computer installation, whenever significant changes are made to the existing computer installation, or at periodic intervals.

Periodic risk analyses are conducted to ensure that safeguards are incorporated commensurate with the value of the computer system and the sensitivity of the unclassified data being processed. Risk Assessments are conducted at least every five years. The CPPM retains a log of all completed Risk Assessments which is used in conjunction with data supplied on Annual Use Certification forms to determine the schedule for Risk Assessment activities. The aim is to reduce risks or losses based on the analysis of the estimated cost, to assess the benefit of protective measures, and to identify the sensitivity of assets requiring protection. A general schedule of required reports and documents is shown in Appendix C.

7.2 Certification and Re-certification

The CPPM reviews each system to determine which applications are sensitive, mission-essential or critical. The review is coordinated with the Computer Operations Manager and the database administrator. The SSCL will re-certify mission-essential items annually. Sensitive applications are then reviewed every three years. Results of these reviews are documented on the Annual Use Certification and Sensitive Questionnaires. Certification of new sensitive applications will be conducted if new requirements for sensitive applications arise.

7.3 Security Awareness and Training Sessions

Computer Security Awareness and Training (CSAT) classroom sessions are provided by Information Services and/or computer security contacts at the time of employee orientations. Security training is presented in on-site training classes. Several levels of CSAT sessions are being developed for different levels of user including Security, Audit, Management and ADP personnel. CSAT sessions will be presented annually. Security memos are sent monthly to update and provide security awareness. Examples of schedules created periodically for computer training and computer security poster distribution are listed in Appendix D.

8.0 REVIEWS

8.1 Compliance Review Results and Recommendations

ADP Management, Data Communications, and Unclassified Computer Security Compliance reviews, are conducted by DOE/CH. Informal, internal compliance reviews will be conducted by the CPPM. Compliance review questionnaires and security level assessment forms are sent to each division and returned to the CPPM for recommendations.

8.2 Security Design Reviews

Security design reviews are performed as sensitive applications are designed or significantly changed.

8.3 System Tests

System tests are conducted as systems are designed or significantly changed. There is no formal, fixed schedule for these reviews. System development efforts are scheduled based on user needs and priorities.

8.4 Risk Assessments

Risk Assessments are reviewed by the CPPM as they are conducted. See Paragraph 7.1 for a description of the Risk Assessment process.

APPENDIX A

APPENDIX A

GLOSSARY

<u>ACPPM</u>	Assistant Computer Protection Program Manager
<u>AD</u>	Associate Director
<u>APPLICATION</u>	computer programs or software which performs a specific function (i.e. payroll, ledger sheet)
<u>CERTIFICATION</u>	reasonable assurance and written acknowledgement made by a CPPM, or individual assigned by the CPPM, that a proposed unclassified computer application processing sensitive information meets all applicable Federal and Departmental policies, regulations, and procedures, and that results of a systems test demonstrate installed security safeguards are adequate and functioning properly.
<u>CIAC</u>	Computer Incident Advisory Capability Information Bulletin.
<u>COMPUTER SECURITY INCIDENT</u>	is the occurrence of an event which has or could adversely affect normal computer operations such as an unauthorized access, interruption to computer service or safeguarding controls, or discovery of a vulnerability.
<u>CPPC</u>	Computer Protection Program Coordinator
<u>CPPM</u>	Computer Protection Program Manager
<u>CRITICAL APPLICATION</u>	are computer programs that must be run on a regular basis in order for the organization or operation to perform its mission or fulfill its contractual obligations. Critical Applications are those that cannot be performed manually and directly affect the Laboratory's mission.
<u>DEC</u>	Digital Equipment Corporation
<u>DOE</u>	Department of Energy
<u>DOE/CH</u>	Department of Energy/Chicago Operations

DOE/SSCPO

Department of Energy/Superconducting Super Collider
Project Office

EPP

Emergency Preparedness Plan

IRM

Information Resources Management

MISSION-ESSENTIAL

is plain text or machine-encoded unclassified data that, as determined by competent authority (e.g., information owners), has high importance related to accomplishing a DOE mission and requires a degree of protection because unnecessary delays in processing could adversely affect the ability of an owner organization, site or the Department to accomplish such missions.

RECERTIFICATION

previously certified unclassified computer application processing sensitive information has been periodically reviewed, that compliance with established protection policies and procedures remains in effect, and that security risks remain at an acceptable level.

SSCL

Superconducting Super Collider Laboratory

SENSITIVE UNCLASSIFIED INFORMATION

is plain text or machine-encoded data that determined by the information owners has relative sensitivity and requires mandatory protection because of statutory or regulatory restrictions or requires a degree of discretionary protection because inadvertent or deliberate misuse, alteration, disclosure, or destruction could adversely affect National or other DOE interests (e.g. data covered under the Privacy ACT Information).

SIGNIFICANT COMPUTER SECURITY INCIDENT

is the occurrence of an event which would be of concern to senior DOE management due to potential for public interest or embarrassment to the organization, or potential for occurring at other DOE sites; these events would include such things as unauthorized access, theft, an interruption to computer service or protective controls, an incident involving damage, a disaster, or discovery of a vulnerability.

APPENDIX B

APPENDIX B

Emergency Contact Teams

Site: Stoneridge Building 4

<u>Emergency Contact Personnel</u>	<u>Phone No.</u>	<u>Pager</u>
Computer Operations		
Brenda Ramsey	(214) 708-6052	(214) 558-6387
Systems Development		
Newell Ramsey	(214) 708-5051	(214) 558-5764
Systems Integration		
Brenda Ramsey Administrative and Scientific VAXES	(214) 708-6052	(214) 558-6387
Brian Scipioni Physics Detector Simulation Facility	(214) 708-5018	
Information Center		
Bruce Dix	(214) 708-5052	(214) 992-8567
Data Network Services & Telecommunications		
Greg Chartrand	(214) 708-5700	(214) 913-3454
Terry Johnson	(214) 708-6085	(214) 781-4552
Computer Security		
Bob Hahn	(214) 708-5055	(214) 558-5960

APPENDIX C

APPENDIX C

COMPUTER SECURITY PROGRAM

MANAGEMENT CONTROL PROCESS SUMMARY

	DISTRIBUTED TO	FREQUENCY
Compliance Review Questionnaires	All Computer Security Contacts & Computing Operations Personnel	Every 2 years*
Installation Security Level Questionnaires	All Computer Security Contacts & Computing Operations Personnel	Every 2 years*
Annual Use certifications AOSS	All Systems except	Every year
Sensitivity Questionnaires AOSS	All Systems except	Every year **
Risk Assessment and Contingency Plans	All Sites	Every 3 years or significant change
AOSS Short Forms	All AOSS users	Every year, based on acquisition date
Sensitive Application Review	User, Programmers	Every 3 years

* Sent with Compliance Review Questionnaires

** Sent with Annual Use Certifications

APPENDIX D

APPENDIX D

Computer Security Awareness

Security Tips

Scheduled To Appear in the SSCL Newsletter

April 1992	Password Security Recommend Practices
May 1992	Sensitive Data
June 1992	Clues to Computer Crime & Abuse
July 1992	Don't Share Password
August 1992	Computer Store
September 1992	It's 5 o'clock — Did you log out?
October 1992	Protecting Disks
November 1992	Backup Data
December 1992	Password Sharing
January 1993	Computer User's Guide
February 1993	Virus Protection
March 1993	Passwords Practices

MEMORANDUM

DATE: Wednesday, April 15, 1992
TO: All Employees
FROM: Tanna Bailey
SUBJECT: Free Computer Training Classes

Here is a listing of the training classes that will be held through the end of May. The classes are free unless otherwise noted. There will be a possibility that in some classes students will share a system. This is due to the enormous demand for training space. **It is important to be prompt for class. If you are not there at the beginning of class your spot will be given to the first person on the waiting list.**

A 24 hour cancellation notice is required to reschedule a student to the next available class. If you are registered for a class and do not show up, your paperwork will be discarded and it will be necessary to re-enroll. Enrollment will be on a "first come first serve" basis. To register please fill out a training registration form and send it to Training MS 1014. *One form per class MUST be filled out.* Please note the classes that are marked (full). Unless there is a cancellation, these classes will not be available for additional students.

The training schedule can be accessed through Public Folder (Zone: LTS1, Folder: tanna) or through Public on QuickMail. The schedule will be updated regularly.

CLASS	DATE	TIME
Mac Orientations - Desktop	April 21	8:30 - 12:30
	April 28 (FULL)	8:30 - 12:30
	May 7	8:30 - 12:30
Beg. Word	April 1 (FULL)	8:30 - 4:30
	May 5	8:30 - 4:30
Int. Word	April 22 (FULL)	8:30 - 4:30
	May 12	8:30 - 4:30
Adv. Word	March 2 (FULL)	8:30 - 4:30
	April 29	8:30 - 4:30
	May 26	8:30 - 4:30
Excel 3.0 Worksheet	April 20 (FULL)	8:30 - 4:30
	April 23 (FULL)	8:30 - 4:30
	May 6	8:30 - 4:30
	May 27	8:30 - 4:30

Excel 3.0 Database/Graphics	March 3 (FULL) April 27 (FULL) May 11	8:30 - 4:30 8:30 - 4:30 8:30 - 4:30
Excel Macro Programming	May 28	8:30 - 4:30
FileMaker Pro	March 30 (FULL)	8:30 - 4:30
Hypercard	scheduled as needed for June	
Wingz I	May 4	8:30 - 4:30
Wingz II	scheduled as needed for June	
Beg. QuickMail	May 7 (FULL)	3:00 - 5:00
Adv. QuickMail	April 21 April 28 (FULL) May 29	3:00 - 5:00 3:00 - 5:00 3:00 - 5:00
Latex	May 8, 15 (FULL) (both days make up one class)	8:30 - 4:30
Canvas 3.0	March 27 (FULL) May 29 (FULL)	8:30 - 12:30 8:30 - 12:30
QuickMail Tips & Tricks	March 3	12:00 - 1:00
Wingz Tips & Tricks	April 7	12:00 - 1:00
Filemaker Pro Tips & Tricks	May 5	12:00 - 1:00
(Brown Bag Lunch Seminar) Bring your own lunch.		
ORACLE DBA (Vax Financials)	March 4-6 (FULL)	Held in the Strategy room
ORACLE PO	March 9 - 13 (FULL)	
ORACLE Financial system administration	March 19 - 20 (FULL)	
ORACLE AP	March 23 - 26 (FULL)	
AFS System Administration	March 4- 6 (FULL) March 16 - 18 (FULL)	8:30 - 4:30 8:30 - 4:30
Beginning UNIX	April 2 - 3	8:30 - 4:30
Intermediate UNIX	May 13 - 14	8:30 - 4:30 Min. charge \$200 per person. May be slightly higher. Cost of class will be evenly distributed between attending students.

X Windows	April 9 - 10	8:30 - 4:30 Min. charge \$200 per person. May be slightly higher. Cost of class will be evenly distributed between attending students.
Fault Tolerant Computing	April 30 - May 1	8:30 - 4:30 Min. charge \$200 per person. May be slightly higher. Cost of class will be evenly distributed between attending students.
Beginning PageMaker	April 24	8:30 - 4:30 Min. charge \$100 per person. May be slightly higher. Cost of class will be evenly distributed between attending students.
C++ Programming	March 16 - 19 (off-site) May 18 - 22 (on-site)	8:30 - 4:30 Min. charge \$500 per person. May be slightly higher. Cost of class will be evenly distributed between attending students.

Attachment 1

(DOE Order 1360.2A)

U.S. Department of Energy
Washington, D.C.

ORDER

DOE 1360.2A

5-20-88

SUBJECT: UNCLASSIFIED COMPUTER SECURITY PROGRAM

1. PURPOSE. To establish requirements, policies, responsibilities, and procedures for developing, implementing, and sustaining a Department of Energy (DOE) unclassified computer security program.
2. CANCELLATION. DOE 1360.2, COMPUTER SECURITY PROGRAM FOR UNCLASSIFIED COMPUTER SYSTEMS, of 3-9-79.
3. SCOPE. The provisions of this Order apply to all Departmental Elements and management and operating contractors as provided by law and/or contract and as implemented by the appropriate contracting officer.
4. APPLICABILITY. Where appropriate, this Order should be used in conjunction with DOE Orders related to telecommunications security and classified computer security. This Order does not apply to classified computer systems used to process or store classified and unclassified information concurrently. In such situations, the provisions of DOE Orders related to classified computer security apply.
5. COVERAGE. This Order covers unclassified computer systems including microcomputers and word processors; it provides for protecting such computer systems and sensitive unclassified automated information and it provides for the continuity of operations of unclassified computer systems and applications that support DOE mission-essential functions.
6. EXCLUSION. In certain situations, other protective measures may already be in place to meet the general requirements but not the specifics contained within this Order. Exceptions from implementing the specifics of this Order may be granted by the managing organization overseeing the site's activities as identified in paragraph 10d of this Order.
7. REFERENCES.
 - a. DOE 1000.2A, INTERNAL CONTROL SYSTEMS, of 6-11-85, which prescribes policies and standards for internal control systems in the Department and assigns responsibilities and accountability to all levels of management for establishing and maintaining effective internal controls to safeguard Departmental resources against theft, fraud, waste, and misuse. (Guidelines on ADP internal controls are available from the Office of Management.)

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of ADP Management

- b. DOE 1330.1A, AUTOMATED MANAGEMENT INFORMATION SYSTEMS AND DATA ADMINISTRATION, of 7-15-83, which establishes policies, responsibilities, and guidelines for the management of automated management information systems (MIS) and the administration of data for use within automated MIS.
- c. DOE 1360.1A, ACQUISITION AND MANAGEMENT OF COMPUTING RESOURCES, of 5-30-86, which establishes Departmental policies and procedures for the acquisition and management of computing resources.
- d. DOE 1800.1A, PRIVACY ACT, of 8-31-84, which establishes guidelines and procedures for implementing Title 5 U.S.C. 552a, the Privacy Act of 1974 in the Department.
- e. DOE 5300.1A, TELECOMMUNICATIONS, of 11-16-81, which establishes policy and general guidance for the use, review, coordination, and provision of telecommunications services for Departmental Elements.
- f. DOE 5300.3B, TELECOMMUNICATIONS: COMMUNICATIONS SECURITY, of 2-12-87, which establishes policy, responsibilities, and guidance concerning the communications security (COMSEC) aspects of the telecommunications services of DOE and implements National policy on telecommunications and automated information systems security.
- g. DOE 5300.4B, TELECOMMUNICATIONS: PROTECTED DISTRIBUTION SYSTEMS, of 9-18-87, which establishes policy and provides guidance concerning protected distribution systems used to transmit classified or sensitive unclassified information related to National security.
- h. DOE 5480 series of Orders pertaining to the physical protection of DOE installations, especially those provisions which deal with fire protection (also see DOE/EP-0108, Standard for Fire Protection of DOE Electronic Computer/Data Processing Systems, of 1-84).
- i. DOE 5500.7A, VITAL RECORDS PROTECTION PROGRAM, of 1-9-87, which establishes the policy and requirements for a program to protect records deemed necessary to assure continuity of essential Government activities.
- j. DOE 5631.5, VIOLATIONS OF LAWS, LOSSES, AND INCIDENTS OF SECURITY CONCERNS, of 2-12-88, which sets forth DOE procedures to assure effective action relating to violations of criminal laws, losses, and incidents of security concern to DOE.
- k. DOE 5635.4, PROTECTION OF UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION, of 2-3-88, which establishes DOE policy and procedures for the protection of unclassified controlled nuclear information.
- l. DOE 5637.1, CLASSIFIED COMPUTER SECURITY PROGRAM, of 1-29-88, which establishes uniform requirements, policies, responsibilities, and procedures for the development and implementation of a DOE Classified Computer Security Program to ensure the security of classified information in automated data processing systems.

5-20-88

- m. Public Law 83-703, "The Atomic Energy Act of 1954," as amended, 42 U.S.C. 2168, which is the statutory basis for the identification and protection of Unclassified Controlled Nuclear Information (UCNI).
 - n. Public Law 99-474, "Computer Fraud and Abuse Act of 1986," which provides for unlimited fines and imprisonment of up to 20 years if a person "intentionally accesses a computer without authorization or exceeds authorized access and, by means of such conduct, obtains information that has been determined...to require protection against unauthorized disclosure...." It is also an offense if a person intentionally accesses "a Federal interest computer without authorization and, by means of one or more instances of such conduct alters, damages, or destroys information...or prevents authorized use of such computer...or traffics any password or similar information...if such computer is used by or for the Government of the United States."
 - o. Public Law 100-235, "Computer Security Act of 1987," which provides for a computer standards program within the National Bureau of Standards, to provide for governmentwide security and to provide for the training in security matters of persons who are involved in the management, operation and use of Federal computer systems, and for other purposes.
 - p. Federal Personnel Manual Letter 732-7, "Personnel Security Program for Position Associated with Federal Computer Systems," which establishes policy for a personnel security program covering positions that are involved in the design, storage, retrieval, access, and dissemination of information maintained in Federal computer systems, as well as positions associated with automated decision-making systems.
 - q. OMB Circular No. A-130, "Management of Federal Information Resources," 12-12-85, which promulgates policy and responsibilities for the development and implementation of computer security programs by executive branch departments and agencies.
 - r. National Security Decision Directive 145, "National Policy on Telecommunications and Automated Information Systems Security," of 9-17-84, which promulgates policy and responsibilities for safeguarding telecommunications and computer systems which transmit or process classified National security information and other sensitive but unclassified information, the loss of which could adversely affect vital interests of the United States.
 - s. National Bureau of Standards (NBS) Publications List 91, "Computer Security Publications," of 2-85, which provides a comprehensive listing of all NBS Federal Information Processing Standards, Guidelines, and Special Publications related to the field of computer security.
8. DEFINITIONS. (See Attachment 1.)

9. POLICY.

- a. DOE unclassified computer systems shall be appropriately protected from abuse and misuse.
- b. Sensitive unclassified automated information shall be appropriately protected from unauthorized access, alteration, disclosure, destruction, or improper use as a result of improper actions or adverse events.
- c. Unclassified computer systems and unclassified computer applications which support DOE mission-essential functions shall be appropriately protected from unnecessary processing delays.
- d. Appropriate security measures shall be utilized, alone or in combination with one another, to protect unclassified computer systems and sensitive unclassified automated information in a cost-effective manner.

10. RESPONSIBILITIES AND AUTHORITIES.

- a. Assistant Secretary, Management and Administration (MA-1), through the Director of Administration (MA-2), has overall authority to:
 - (1) Promulgate Departmental policies, procedures, and guidelines related to the requirements of this Order: and
 - (2) Apprise Heads of Field Elements of results of program management reviews conducted in response to the requirements of this Order and make recommendations for improvement, as appropriate.
- b. Director of ADP Management (MA-24) shall:
 - (1) Develop and coordinate the implementation of Departmental policies, procedures, and guidelines related to the requirements of this Order.
 - (2) Serve as the Departmental point of contact on sensitive unclassified automated information and unclassified computer security matters.
 - (3) Coordinate the review and dissemination of information concerning significant unclassified computer security incidents.
 - (4) Conduct program management reviews of appropriate Field Elements, as identified in paragraph 10d, to assess the sustained effectiveness of their management oversight of the unclassified computer security programs established by sites under their cognizance and make recommendations to MA-2 for improvement, as appropriate.
 - (5) Coordinate development of DOE policy and procedures for the unclassified computer security program with the Office of Safeguards and Security as they relate to the classified computer security

program and related security matters and with the Office of Computer Services and Telecommunications Management for unclassified telecommunications security.

- c. Director of Computer Services and Telecommunications Management (MA-25) shall:
- (1) Develop and implement Departmental policies, procedures, and guidelines for protecting the transmission of sensitive unclassified information and protecting unclassified telecommunications resources from misuse and abuse.
 - (2) Coordinate development of DOE policies, procedures, and guidelines protecting the transmission of sensitive unclassified information to the Office of ADP Management.
- d. Managers of Operations Offices or the Office of ADP Management (MA-24) (Office of ADP Management has the following responsibilities for sites not reporting through an operations office), shall:
- (1) Designate an individual knowledgeable in both computing and computer security methods and practices to be the Computer Protection Program Coordinator (CPPC). The CPPC shall serve as a focal point to coordinate activities in this Order between the Office of ADP Management and the individual sites.
 - (2) Implement and coordinate an appropriate management oversight procedure which ensures awareness and compliance with this Order at cognizant DOE and DOE contractor sites.
 - (3) Ensure that each DOE and DOE contractor site under their cognizance establishes, implements, and sustains a computer protection program in accordance with the requirements of this Order.
 - (4) Schedule and conduct periodic compliance reviews at cognizant sites to assess the adequacy of computer protection plans and the sustained effectiveness of the computer security program procedures and to make recommendations for improvement, as appropriate. Compliance reviews should be conducted every 2 or 3 years based upon reviewing management's judgment. Factors to be considered in making this decision include reviewing management's perception of the sensitivity and/or value of the information or other assets to be protected at each site.
 - (5) Ensure that procedures are implemented for identifying unclassified computer security incidents that occur at sites under their cognizance. These procedures shall ensure that significant unclassified computer security incidents are reported to the Office of ADP Management immediately following detection of the incident and

that significant incident information received from Headquarters is disseminated to cognizant sites. (Procedures are described in Attachment 2.)

- (6) Ensure that information related to the unclassified computer security program (e.g., information describing specific vulnerabilities or protection features) is provided protection commensurate with the sensitivity of that information when it is collected, stored, or distributed.
- (7) Ensure that, through the contracting officer, all appropriate contractors are required to comply with the provisions of this Order.
- (8) Grant exceptions from implementing specific requirements of this Order. (See page 1, paragraph 6.)
- (9) Coordinate requirements of this Order, and related computer security matters, with organizations/individuals having responsibilities for telecommunications security and classified computer security.

11. REQUIREMENTS.

- a. The site (DOE or contractor) manager will assure that a management official, knowledgeable in both computing and computer security methods and practices, is designated as the Computer Protection Program Manager (CPPM). In cases where multiple computer installations, computer systems, or program-area applications exist, the CPPM may designate assistant CPPM's to accomplish specific security responsibilities.
- b. The CPPM shall:
 - (1) Implement and administer a management control process appropriate to the environment of the site to ensure that the sensitivity and/or essentiality of the information processed on a computer is determined by the owners of automated information and that appropriate administrative, technical, physical, and personnel protection measures and procedures are incorporated into all new and operational unclassified computer systems and unclassified computer applications processing sensitive information to achieve and sustain an acceptable level of security. (See paragraph 11c for description of this management control process.)
 - (2) Formulate, continually update, and annually review a computer protection plan which will allow the appropriate approving (i.e., site management) or reviewing (e.g., an operations office) authorities to judge the comprehensiveness and effectiveness of the computer protection program. In cases where multiple computer installations, computer systems, or program-area applications exist, multiple plans may be appropriate. (See paragraph 11d for a description of the required contents of a computer protection plan.)

5-20-88

- (3) Develop and implement procedures establishing controls designed to prevent misuse and abuse of unclassified computer resources. (See paragraph 11e for a description of controls.)
 - (4) Develop and implement a process, as appropriate, for providing contingency planning and reasonable continuity of operations for unclassified computer systems and unclassified computer applications supporting mission-essential functions in the event of a disruption to normal operations. (See paragraph 11h for a description of this process.)
 - (5) Develop and implement procedures for reporting significant unclassified computer security incidents, as described in Attachment 2.
 - (6) Ensure that plans are developed and implemented for conducting continuous computer security awareness and training to assure that DOE and DOE contractor personnel involved in managing, designing, developing, operating, maintaining unclassified computer applications processing sensitive information, and who use unclassified computer systems are aware of their security responsibilities, know how to fulfill them, are kept aware of vulnerabilities, and are trained in techniques to enhance security.
 - (7) Coordinate the requirements of this Order and related computer security matters with organizations/individuals having responsibilities for telecommunications security and classified computer security.
- c. The management control process must ensure that the following, as a minimum, are carried out:
- (1) Periodic risk assessments are conducted for new and existing computer installations to ensure that appropriate, cost-effective safeguards are incorporated commensurate with the sensitivity and value of associated computer systems, computer applications, and unclassified information processed. (See paragraph 11f for description of risk assessment process.)
 - (2) Procedures are established for defining functional security requirements, developing security specifications, conducting security design reviews and system tests, certifying and recertifying unclassified computer applications processing sensitive information at appropriate phases of the systems life cycle, and approving security specifications for the acquisition of computer resources related services. (See paragraph 11g for minimum security requirements.)

- (3) Personnel who participate in managing, designing, developing, operating, or maintaining unclassified computer applications processing sensitive information, or who access automated sensitive unclassified information, are appropriately screened to a level commensurate with the sensitivity of the data to be accessed or handled and the risk and magnitude of loss or harm that could be caused by the individual. Federal personnel are to be screened in accordance with the Office of Personnel Management policies and procedures. (Guidelines on screening non-Federal personnel are available from the Office of ADP Management.)
 - (4) Appropriate protection measures are established, to the extent economically and technically feasible, for maintaining personal accountability of individual users granted access to sensitive unclassified automated information, and that they have access to no more information than authorized.
 - (5) Followup procedures are in place to ensure implementation of protective measures in accordance with recommendations from compliance review and certification/recertification review activities.
 - (6) Appropriate installation disaster recovery plans and application contingency plans are established and maintained for computer installations and applications supporting DOE mission-essential functions to prevent loss of information, minimize interruption, and provide reasonable continuity of computer services should adverse events occur that would prevent normal operations.
 - (7) Computer protection plans are approved by appropriate management officials.
1. The computer protection plan must be kept current and should include elements that are relative to the coverage of the plan and to the environment of the site, as follows:
- (1) Summary of the management control process describing the administrative, technical, physical, and personnel safeguards employed at the site. If special provisions apply to selected computer systems or applications, this information should be included.
 - (2) Reference to list(s) which uniquely identify the unclassified computer applications that process sensitive information, the owners of such applications, and the unclassified computer systems which provide processing support.
 - (3) Reference to contingency and disaster recovery plans.

- (4) Reference to schedules indicating planned and completed risk assessments, certification/recertifications, compliance reviews, audits, inspections or management reviews, and security awareness and training sessions. Schedules should, at a minimum, indicate the fiscal year planned for such tasks.
 - (5) Reference to documents containing the results of the latest compliance review, risk assessments, security design reviews, system tests, certifications/recertifications, and followup actions on previous recommendations from these review activities.
 - (6) Reference to a plan for continually providing security awareness and training to personnel who manage, design, develop, operate, maintain or use unclassified computer systems. Plans for onsite personnel should include, as a minimum, training schedule, type of training, personnel attending, and date of attendance. Plans for off site users may be less specific and describe approaches for disseminating security awareness and training information.
 - (7) Identification of software tools used to enhance security.
 - (8) Reference to the procedure for identifying computer security incidents and reporting significant incidents.
 - (9) Reference to lists which identify CPPM, assistant CPPM's, computer security incident response personnel (e.g., management of installation, operations, users), emergency response personnel (e.g. building maintenance, building protective service, fire department), and locations where they may be contacted.
- e. In addition to appropriate administrative, technical, physical, and personnel protective measures, controls to prevent misuse and abuse of unclassified computer resources should include the following:
- (1) Developing and implementing a procedure, where feasible, to maintain automated computer systems logs of accesses to multiuser computer systems to determine whether unauthorized accesses are being attempted.
 - (2) Reviewing the contents of unclassified computer system files at unannounced intervals and by means of random sampling.
 - (3) Developing and implementing procedures requiring all personnel who access unclassified computer systems to have a working knowledge of unclassified computer security responsibilities, policies, procedures, and administrative or legal actions which may be pursued for computer security incidents or violations of related laws.
 - (4) Ensuring that all actions constituting suspected or confirmed unclassified computer security incidents are brought to the immediate

attention of the appropriate CPPM; that the extent and cause of any incidents are determined; and that reasonable steps are taken to minimize the probability of further occurrence including counseling, disciplinary actions, and/or notifying criminal investigative and law enforcement authorities, as appropriate.

- f. The risk assessment process must ensure, as a minimum, the following:
- (1) A risk assessment methodology is selected (i.e., quantitative and/or qualitative) which includes the following elements, as appropriate:
 - (a) Determination of risk assessment scope. For example, a risk assessment at a large installation may include all hardware or be limited to an assessment of an individual mainframe or microcomputer system. Regardless of the approach, the scope of the risk assessment should be maintained within manageable limits and the level of effort commensurate with the nature of the installation being assessed (e.g., risk assessment of a stand-alone microcomputer installation should be a less formal review and the responsibility of user management).
 - (b) Identification of major computer installation assets and general approximations of their current replacement value in order to establish a basis for making decisions on protective measures as described in paragraph 11f(1)(g) below.
 - (c) General determination of collective sensitivity and/or value of information processed or stored at the installation and potential impacts if information is misused, altered, destroyed, or disclosed. This determination should be based on an analysis of individual functional security requirements of unclassified computer applications processed.
 - (d) Identification of existing protective measures.
 - (e) Identification of existing and potential threats and hazards, and quantitative estimates of loss expectancy or qualitative levels of risk exposure to possible adverse events.
 - (f) Determination of acceptable loss expectancies or risk exposures, or determination of alternative protective measures and associated costs for reducing loss expectancies or risk exposures to acceptable levels.
 - (g) Recommendations for accepting loss expectancies or risk exposures, or recommendations of appropriate protective measures for improving security (reducing risks or loss expectancy) based on analysis of the ratio between the estimated cost and benefit of proposed protective measures and the value/sensitivity of

5-20-88

assets requiring protection. The cost of protective measures should not normally exceed a reasonable percentage of the value of assets requiring protection (as identified in paragraphs 11f(1)(b) and 11f(1)(c) above).

- (h) Documentation of actions taken or planned as a result of the risk assessment findings and recommendations.
 - (i) Followup procedures to ensure that all actions planned have been carried out.
- (2) Risk assessments are performed:
- (a) Prior to construction or operational use of a new computer installation.
 - (b) Whenever there is a significant change to the existing computer installation.
 - (c) At periodic time intervals, established by the CPPM, which are commensurate with the sensitivity of the information process by the computer installation, but not to exceed 5 years if no risk assessment has been performed during that time.
- (3) Selected risk assessment methodologies and results are approved by appropriate management officials (e.g., installation level or site level) and taken into consideration when certifying or recertifying unclassified computer applications processing sensitive information.
- (4) Risk assessment results are available for consideration during the evaluation of internal controls, conducted in accordance with DOE 1000.3A, that apply to computer installation or unclassified applications processing sensitive information.
- g. To meet security requirements that protect sensitive unclassified information, the following, as a minimum, are required:
- (1) For new or significantly changed computer applications that process sensitive unclassified information that:
 - (a) Functional security requirements are defined by information owners and should be based on established procedures which include the following:
 - Determining the nature of the sensitivity of information to be processed, and how the application/information may be vulnerable (e.g., to misuse, alteration, destruction, or disclosure).

- 2 Determining potential impacts if sensitive information is misused, altered, destroyed, or disclosed.
- (b) Security specifications are developed by system designers which detail functional security requirements and describe how specific protective techniques will be employed in technical terms that programmers and system developers can implement;
 - (c) Functional security requirements and security specifications are reviewed and approved prior to acquiring or starting formal development;
 - (d) Results of risk assessments performed at the computer installation where the computer application will be processed are taken into consideration when defining and approving security specifications for computer applications;
 - (e) Security design reviews and system tests are conducted and approved prior to operational use of unclassified computer applications; and
 - (f) Upon successful completion of the system test, the unclassified computer application is certified as meeting requirements of documented and approved security specifications and related applicable Federal and Departmental policies, regulations and standards, and that results of the system test demonstrate that application, computer system, and installation protective measures are adequate and functioning properly.
- (2) For operational computer applications processing sensitive unclassified information that:
- (a) Periodic reviews are conducted and recertifications are made of the protection adequacy and proper functioning of protection measures;
 - (b) The recertification process takes into consideration all available information, including other reviews conducted; and
 - (c) Recertifications are conducted at least every 3 years or more frequently, as appropriate. Time intervals should be commensurate with the sensitivity of the information processed. If no significant change has taken place and no deficiencies have been indicated in other review activities, the recertification process may be less stringent than the initial certification process.

- (3) For the acquisition of equipment and software, or contracts for the operation of unclassified computer installations or related services that:
 - (a) Appropriate functional security requirements are incorporated into security specifications;
 - (b) Functional security requirements and security specifications are reasonably sufficient for the intended application; that they comply with current Federal computer security policies, procedures, and standards; and that installation protection provisions are adequate and functioning properly prior to operational use; and
 - (c) Resource-sharing service agreements provide for compliance with applicable provisions of this Order by responsible management officials at the processing site.
- h. As appropriate, disaster recovery plans for unclassified computer installations and contingency plans for applications supporting mission-essential functions should provide for minimizing interruption and a reasonable continuity of services should adverse events occur that prevent normal operations. This includes the following:
 - (1) Identifying which applications support mission-essential functions.
 - (2) Determining potential impacts should unnecessary processing delays occur.
 - (3) Determining when an application that supports a mission-essential function must be back in operation after an interruption to avoid adversely affecting the mission of the user or the owner organization.
 - (4) Determining the relative importance of the application to the overall mission of the installation, the site, or the Department. The relative importance should be based on the essentiality rating assigned to those applications deemed essential by the owner organization.
 - (5) Determining the appropriate amount of documentation. The amount of documentation detailed in these plans should be commensurate with the nature of the computer installation (e.g., documented in more detail for large complex computer installations supporting multiuser computer systems and documented in less detail for small installations supporting single-user computer systems).
 - (6) Determining test intervals and providing reasonable assurance that recovery requirements can be met. Plans should be operationally tested during initial systems tests and at time intervals commensurate

5-20-88

with the associated risk of harm or loss. Formal written agreements shall be established to ensure that sufficient processing capacity and time will be available especially to meet the recovery requirements of mission essential computer applications when backup processing at alternate computer installations is considered necessary.

- (7) Identifying key individuals and developing proper emergency notification procedures.

BY ORDER OF THE SECRETARY OF ENERGY:



LAWRENCE F. DAVENPORT
Assistant Secretary
Management and Administration

DEFINITIONS

1. AUTOMATED INFORMATION refers to all recorded information regardless of its media form (e.g., audible tone; paper; magnetic core, tape, or disk; microform electronic signal; and visual/screen displays) that is processed by or stored for the purpose of being processed by a computer system. The terms "automated information", "automated data", "information", and "data" are considered synonymous and used interchangeably in this Order.
2. CERTIFICATION is a reasonable assurance (based on a technical evaluation of a system test) and written acknowledgment made by a CPPM, or an individual designated by the CPPM, that a proposed unclassified computer application processing sensitive information meets all applicable Federal and Departmental policies, regulations, and procedures, and that results of a systems test demonstrate installed security safeguards are adequate and functioning properly.
3. COMPLIANCE REVIEW refers to a review and examination of records, procedures, and review activities at a site in order to assess the unclassified computer security posture and ensure compliance with this Order. This review is normally conducted by the CPPC at an operations office having cognizance over the site and management responsibilities for implementing this Order. For those sites not reporting to an operations office, this review is normally conducted by the Office of ADP Management.
4. COMPUTER INSTALLATION is the physical space which contains one or more computer systems. Computer installations may range from locations for large centralized computer centers to locations for individual stand-alone microcomputers.
5. COMPUTER PROTECTION PLAN is a document which serves as the single source management summary of information associated with the DOE unclassified computer security program as required on page 8, under paragraph 11d. It serves as a basis for estimating security needs, performing security assessments, performing compliance and management reviews, and facilitating risk management and certification efforts.
6. COMPUTER SECURITY INCIDENT is the occurrence of an event which has or could adversely affect normal computer operations such as an unauthorized access, interruption to computer service or safeguarding controls, or discovery of a vulnerability.
7. COMPUTER SITE is a geographic location where one or more computer installations is managed and operated.
8. CONTINGENCY PLANS are documents, developed in conjunction with computer application owners and maintained at the primary and backup computer installation; they describe procedures and identify personnel necessary to respond to abnormal situations, and ensure that computer application owners can continue to process mission-essential applications in the event that computer support is interrupted (e.g., appropriate automated and/or manual backup processing capabilities).

9. DISASTER RECOVERY PLANS are documents containing procedures for emergency response, extended backup operations, and post-disaster recovery should a computer installation experience a partial or total loss of computer resources and physical facilities. The primary objectives of these plans, in conjunction with contingency plans, are to provide reasonable assurance that a computer installation can recover from such incidents, continue to process mission-essential applications in a degraded mode (i.e., as a minimum, process computer applications previously identified as most essential), and return to a normal mode of operation within a reasonable amount of time. Such plans are a protective measure generally applied based on assessments of risk, cost, benefit, and feasibility as well as the other protective measures in place.
10. ESSENTIALITY RATING is an importance-time-related designation assigned to a computer application that indicates when an application must be back in operation to avoid mission impacts after a disaster or interruption in computer support services at a multiuser installation. To facilitate prioritized recovery procedures and for operating at offsite backup facilities in a degraded mode (i.e., only most essential applications), computer applications should be assigned essentiality ratings of varying importance (e.g., most essential, essential, important, deferrable). Applications with the same essentiality rating (i.e., most essential) should be additionally ranked (e.g., numerically) according to installation or site determined processing priorities and perceptions of importance.
11. MANAGEMENT REVIEW refers to a review and examination of records, activities, policies, and procedures established by operations offices and other designated offices to manage and coordinate unclassified computer security programs which are established by sites under their cognizance. This review is normally conducted by Headquarters personnel with Departmental program management responsibilities.
12. MISSION-ESSENTIAL UNCLASSIFIED INFORMATION is plain text or machine-encoded unclassified data that, as determined by competent authority (e.g., information owners), has high importance related to accomplishing a DOE mission and requires a degree of protection because unnecessary delays in processing could adversely affect the ability of an owner organization, site, or the Department to accomplish such missions.
13. PERSONNEL SCREENING is a protective measure applied to determine that an individual's access to sensitive unclassified automated information is admissible. The need for and extent of a screening process is normally based on an assessment of risk, cost, benefit, and feasibility as well as other protective measures in place. Effective screening processes are applied in such a way as to allow a range of implementation, from minimal procedures to more stringent procedures commensurate with the sensitivity of the data to be accessed and the magnitude of harm or loss that could be caused by the individual. (Guidelines on screening non-Federal employees are available from the Office of ADP Management.)

14. PROTECTIVE MEASURES are physical, administrative, personnel, and technical security measures which, when applied separately or in combination, are designed to reduce the probability of harm, loss or damage to, or compromise of an unclassified computer system or sensitive and/or mission-essential information.
15. RECERTIFICATION is an ongoing reassurance that a previously certified unclassified computer application processing sensitive information has been periodically reviewed, that compliance with established protection policies and procedures remains in effect, and that security risks remain at an acceptable level.
16. RISK ASSESSMENT is a management tool which provides a systematic approach for determining the relative value and sensitivity of computer installation assets, assessing vulnerabilities, assessing loss expectancy or perceived risk exposure levels, assessing existing protection features and additional protection alternatives or acceptance of risk, and documenting management decisions. Decisions for implementing additional protection features are normally based on the existence of a reasonable ratio between cost/benefit of the safeguard and sensitivity/value of the assets to be protected. Risk assessments may vary from an informal review of a small scale microcomputer installation to a more formal and fully documented analysis (i.e., risk analysis) of a large scale computer installation. Risk assessment methodologies may vary from qualitative or quantitative approaches to any combination of these two approaches.
17. SECURITY DESIGN REVIEW is a review process where the objective is to ascertain that implemented protective measures meet the original overall system design and approved computer application security requirements. The security design review may be a separate activity or an integral function of the overall application system design review activity.
18. SENSITIVE UNCLASSIFIED INFORMATION is plain text or machine-encoded data that, as determined by competent authority (e.g., information owners), has relative sensitivity and requires mandatory protection because of statutory or regulatory restrictions (e.g., Unclassified Controlled Nuclear Information, Official Use Only information, Privacy Act Information) or requires a degree of discretionary protection because inadvertent or deliberate misuse, alteration, disclosure, or destruction could adversely affect National or other DOE interests (e.g., program critical information, or controlled scientific and technical information which may include computer codes (computer programs) used to process such information).
19. SIGNIFICANT CHANGE refers to a change in an unclassified computer installation which could impact overall processing requirements and conditions or installation security requirements (e.g., adding a local area network; changing from batch to online processing; adding dial-up capability; carrying out major hardware configuration upgrades; operating system changes; making major change to the physical installation; or changing installation location).

20. SIGNIFICANT COMPUTER SECURITY INCIDENT is the occurrence of an event which would be of concern to senior DOE management due to potential for public interest or embarrassment to the organization, or potential for occurring at other DOE sites; these events would include such things as unauthorized access, theft, an interruption to computer service or protective controls, an incident involving damage, a disaster, or discovery of a vulnerability.
21. UNCLASSIFIED TELECOMMUNICATIONS SECURITY is that domain of unclassified computer security that is concerned with protecting the point-to-point communication (e.g., input device to computer, computer to computer) of sensitive unclassified information with appropriate cost-effective measures (e.g., data encryption and protected distribution systems). Such communications generally occur via data communication systems, links, and devices such as networks, local area networks, telephone/wire lines, fiber optics, radio waves/microwaves, and integrated circuits.

PROCEDURE FOR REPORTING SIGNIFICANT
UNCLASSIFIED COMPUTER SECURITY INCIDENTS

1. GENERAL.

- a. This procedure has been developed as a method for timely reporting of significant unclassified computer security incidents, for determining the type of information to be reported, and for appropriate follow-on activities after the initial notification of an incident.
- b. Reports of significant unclassified computer security incidents will be used to alert sites to computer system vulnerabilities, unauthorized access to computer systems, and other problems which could adversely affect DOE or an DOE contractor computer site. Through sharing of incident information, vulnerabilities can be identified, computer security awareness can be elevated, and risks can be reduced. The timely reporting of significant computer security incidents will also serve to alert management to situations which might receive public attention.

2. ELEMENTS OF A SIGNIFICANT INCIDENT REPORTING PROCEDURE. This procedure provides necessary steps for reporting significant computer security incidents at sites which have implemented, or are in the process of implementing, the unclassified computer security program. Use of this procedure should complement and be compatible with incident reporting procedures for classified systems where there may be mutual security program concerns (e.g., a hardware or system-software-related incident which is peculiar to a specific vendor and may affect both classified and unclassified systems).

- a. Immediately after detection of an unclassified computer security incident deemed significant, the Computer Protection Program Manager (CPPM) shall notify the appropriate operations/oversight office. The operations/oversight office shall then notify the Office of ADP Management. The ultimate objective of this notice is to alert other sites to potential problems that may have an impact on them and should provide the following information:
 - (1) A general description of what has happened;
 - (2) Characterization of perpetrator(s) thought to be involved (i.e., insider, outsider); and
 - (3) What corrective actions have been taken or are planned.
- b. The CPPM, in consultation with the CPPC, as appropriate, should determine what type of support (e.g., legal counsel, security, classification, law enforcement) is required. Names and telephone numbers of persons contacted in other organizations should be maintained and included in follow-on reports. Should a classification review determine the incident

5-20-88

affects classified computer systems and is, therefore, classified, all communications between the site, operations office, and Headquarters shall be through classified channels.

- c. After all applicable information has been obtained, a written follow-on report shall be forwarded, through the same DOE channels, to the Office of ADP Management. This follow-on report should contain the following information, as appropriate:
 - (1) Date and time of incident;
 - (2) Location of incident: computer installation and/or appropriate identification of hardware and software;
 - (3) Nature of the incident:
 - (a) What caused the incident; and
 - (b) Characterization of perpetrator(s) thought to be involved (i.e., insider, outsider);
 - (4) Effects of incident:
 - (a) Organizational element affected; and
 - (b) What is affected (e.g., installation, hardware, communication networks, software (including version number));
 - (5) Corrective actions taken or planned;
 - (6) Law enforcement, legal counsel, security, and classification contacts made, if appropriate;
 - (7) What implications does this incident have for other sites, if any;
 - (8) Recommendations concerning the following:
 - (a) Assistance needed by the site;
 - (b) Need to change or establish new laws, regulations;
 - (c) Additional action that should be taken by higher authorities; and
 - (9) Name and telephone number of CPPM.
- d. A copy of these significant unclassified computer security incident reports should be retained by the site. The retention period for these records should be determined by the CPPM. Factors to be considered in determining this retention period include the need for availability of this information during periodic security reviews, risk assessments, trend analysis activities.

Attachment 2

(SSC Distributed Systems)

SUPERCONDUCTING SUPER COLLIDER COMPUTING RESOURCES

March 13, 1992

55

