THIS PAGE MUST BE KEPT WITH DOE 1360.2B, UNCLASSIFIED COMPUTER SECURITY PROGRAM.

DOE 1360.2B, UNCLASSIFIED COMPUTER SECURITY PROGRAM, HAS REVISED DOE 1360.2A TO REFLECT ORGANIZATIONAL TITLE, ROUTING SYMBOL, AND OTHER EDITORIAL REVISIONS REQUIRED BY SEN-6. NO SUBSTANTIVE CHANGES HAVE BEEN MADE. DUE TO THE NUMBER OF PAGES AFFECTED BY THE REVISIONS, THE ORDER HAS BEEN ISSUED AS A REVISION.

U.S. Department of Energy

Washington, D.C.

ORDER

DOE 1360.2B

5-18-92

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 (UCS) program.

2. CANCELLATION. DOE 1360.2A, UNCLASSIFIED COMPUTER SECURITY PROGRAM of 5-20-88.

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 10c of this Order.

7. REFERENCES. See Attachment 1.

8. DEFINITIONS. See Attachment 2.

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.

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Information Resources Management

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. Director of Administration and Human Resource Management (AD-1) through the Director of Information Resources Management (AD-20), shall:

(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 Information Resources Management (AD-20), through the Director of IRM Policy, Plans, and Oversight (AD-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 UCS matters.

(3) Coordinate the review and dissemination of information concerning significant UCS incidents.

(4) Conduct program management reviews of appropriate field elements, as identified in paragraph 10c, to assess the sustained effectiveness of their management oversight of the UCS programs established by sites under their cognizance and make recommendations to AD-20 for improvement, as appropriate.

(5) Coordinate development of DOE policy and procedures for the UCS program with the Office of Security Affairs as they relate to the classified computer security program.

(6) 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.

(7) Ensure that procedures are developed with each Lead Program Secretarial Officer which describes the process for interface and communicating with the DOE Field Offices.

c. Managers of DOE Field Offices or AD-24, as appropriate (AD-24 has the following responsibilities for sites not reporting through a DOE Field 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 AD-24 and the individual sites.

(2) Implement and coordinate an appropriate management oversight process 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 (CPP) 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 UCS incidents that occur at sites under their cognizance. These procedures shall ensure that significant UCS incidents are reported to AD-24 immediately following detection of the incident and that significant incident information received from Headquarters is disseminated to cognizant sites. (Procedures are described in Attachment 3.)

(6) Ensure that information related to the UCS 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 1lc, below, for description of this management control process.)

(2) Formulate, continually update, and annually review a CPP which will allow the appropriate approving (i.e., site management) or reviewing (e.g., a DOE Field 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, below, for a description of the required contents of a CPP.)

(3) Develop and implement procedures establishing controls designed to prevent misuse and abuse of unclassified computer resources. (See paragraph he, below, for a description of control s.)

(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, below, for a description of this process.)

(5) Develop and implement procedures for reporting significant UCS incidents, as described in Attachment 3.

(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, below, 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 or related services. (See paragraph 11g, below, 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 AD-24.)

(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 (DRP) 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) CPPs are approved by appropriate management officials.

d. The CPP 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 plans and DRPs.

(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 offsite 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 CPPMs, 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 leas 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 UCS 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 UCS 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 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 is commensurate with the sensitivity of the information processed 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 1000.3B, 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:

1 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 recertification 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) Recertification 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, DRPs for unclassified computer installations and contingency plans for applications supporting mission-essential functions should provide for minimizing interruption and 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 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:

DONALD W. PEARMAN, JR.
Acting Director
Administration and Human
Resource Management

REFERENCES

1. DOE 1000.3B, INTERNAL CONTROL SYSTEMS, of 7-5-88, 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 automatic data processing (ADP) internal controls are available from the Office of IRM Policy, Plans, and Oversight (AD-24).)

2. DOE 1330.1D, COMPUTER SOFTWARE MANAGEMENT, of 5-18-92, 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.

3. 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.

4. 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.

5. DOE 5300.1C, TELECOMMUNICATIONS, of 6-12-92, which establishes policy and general guidance for the use, review, coordination, and provision of telecommunications services for Departmental Elements.

6. DOE 5300.3C, TELECOMMUNICATIONS: COMMUNICATIONS SECURITY, of 5-18-92, 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.

7. DOE 5300.4C, TELECOMMUNICATIONS: PROTECTED DISTRIBUTION SYSTEMS, of 5-18-92, which establishes policy and provides guidance concerning protected distribution systems used to transmit classified or sensitive unclassified information related to national security.

8. 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).

9. DOE 5500.7B, EMERGENCY OPERATING RECORDS PROTECTION PROGRAM, of 10-23-91, which establishes the policy and requirements for a program to protect records deemed necessary to assure continuity of essential Government activities.

10. DOE 5639.3, VIOLATIONS OF LAWS, LOSSES, AND INCIDENTS OF SECURITY CONCERNS, of 9-15-92, which sets forth DOE procedures to assure effective action relating to violations of criminal laws, losses, and incidents of security concerns to DOE.

11. 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.

12. DOE 5639.6, CLASSIFIED COMPUTER SECURITY PROGRAM, of 9-15-92, 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 ADP systems.

13. 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).

14. 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."

15. Public Law 100-235, "Computer Security Act of 1987," which provides for a computer standards program within the National Institute of Standards and Technology (NIST), 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.

16. 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.

17. Office of Management of Budget (OMB) Circular No. A-130, "Management of Federal Information Resources," of 12-12-85, which promulgates policy and responsibilities for the development and implementation of computer security programs by executive branch departments and agencies.

18. 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.

19. NIST Publications List 91, "Computer Security Publications," of 2-85, which provides a comprehensive listing of all NIST Federal Information Processing Standards, guidelines, and special publications related to the field of computer security.

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 Computer Protection Program Manager (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 (UCS) posture and ensure compliance with this Order. This review is normally conducted by the Computer Protection Program Coordinator (CPPC) at a DOE Field Office having cognizance over the site and management responsibilities for implementing this Order. For those sites not reporting to a DOE Field Office, this review is normally conducted by the Office of IRM Policy, Plans, and Oversight (AD-24) .

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 Department of Energy (DOE) UCS program as required on page 6, 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 multi user 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 DOE Field Offices and other designated offices to manage and coordinate UCS 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 AD-24.)

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 on-line 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 UCS 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 (UCS) INCIDENTS

1. GENERAL .

   a. This procedure has been developed as a method for timely reporting of significant UCS 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 UCS incidents will be used to alert sites to computer system vulnerabilities, unauthorized access to computer systems, and other problems which could adversely affect Department of Energy (DOE) or any 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 UCS 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 UCS incident deemed significant, the Computer Protection Program Manager (CPPM) shall notify the appropriate DOE Field Office. The DOE Field Office shall then notify the Office of IRM Policy, Plans, and Oversight (AD-24). 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 Computer Protection Program Coordinator, 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

affects classified computer systems, and is therefore classified, all communications between the site, DOE Field 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 AD-24. 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 UCS 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, and trend analysis activities.