DE

ANL/TM--458-Rev.3

DE92 004704

ANL Statement of Site Strategy for Computing Workstations

By

L. Michael Boxberger
Lawrence W. Amiot
Miriam E. Bretscher
Douglas E. Engert
Fred M. Moszur
Charles J. Mueller
Diane E. O'Brien
C. Gary Schlesselman
L. Jean Troyer

Edited by

Karen R. Fenske

November 1991

Computing and Telecommunications Division
Argonne National Laboratory, 9700 South Cass Avenue, Argonne, Illinois 60439-4801

(Intended primarily for internal distribution)

ACKNOWLEDGMENTS

The ANL Computing Policy Committee (CPC), The Computing and Telecommunications Division (CTD), the Electronics Department (EL), and the Procurement Department (PRO) have developed a Laboratory strategy for computing workstations and reviewed the *ANL Statement of Site Strategy for Computing Workstations* (ANL/TM 458, Revision 3) as a current reflection of that strategy.

The authors of the *Site Strategy* have also served as management/staff reviewers of the document. Other CTD reviewers were Clifford M. Caruthers, senior CTD editor, and David P. Weber, Director of CTD, who provided the overall guidance to ensure that the final product would accurately represent the Laboratory's strategy for computing workstations.

PREFACE

The *ANL Statement of Site Strategy for Computing Workstations* (ANL/TM 458, Revision 3) is one of several contributions to the DOE information technology resources planning and reporting process. Argonne National Laboratory has prepared this *Site Strategy* according to DOE Order 1360.1A as issued May 30, 1986, by the DOE Director of Administration.

The *Site Strategy* consists of seventeen chapters that together explain the overall Argonne strategy for defining, acquiring, using, and evaluating computing workstations and other automated office support systems. Appendices A, B, F, and G clarify Argonne's responsibilities in managing microprocessors and word processors and in acquiring computing workstation components. Appendix C contains the "ANL Network Management Policy Statement," Appendix D contains the "ANL Computer Protection Policy," Appendix E contains the "ANL Procedure for Reporting Computer Security Incidents," and Appendix H contains a document titled "Use of Computers at Argonne National Laboratory," which all new employees must sign, confirming their understanding of and responsibility for using computers at ANL.

For a summary of word processors, personal computers, workstations, and associated software, see the *Survey of ANL Organization Plans for Word Processors, Personal Computers, Workstations, and Associated Software* (ANL/TM 459, Revision 3). As a companion document to the *Site Strategy*, this *Survey* describes the plans of each organization for scientific workstations, personal computing, local area networking, and office automation. The *Survey* also identifies appropriate planners and other contact people in those organizations, and promotes the sharing of this information among those people making plans for organizations and decisions about acquiring equipment and software and implementing applications.

CONTENTS

TABLES

FIGURES

CHAPTER 1

INTRODUCTION

This *Statement of Site Strategy* describes the procedure at Argonne National Laboratory for defining, acquiring, using, and evaluating scientific and office workstations and related equipment and software in accord with DOE Order 1360.1A (5-30-86), and Laboratory policy.

It is Laboratory policy (1) to promote the installation and use of computing workstations to improve productivity and communications for both *programmatic and support personnel*, (2) to ensure that computing workstation acquisitions meet the expressed need in a cost-effective manner, and (3) to ensure that acquisitions of computing workstations are in accord with Laboratory and DOE policies (see Appendix A).

The overall computing site strategy at ANL is to develop a hierarchy of integrated computing system resources to address the current and future computing needs of the Laboratory. The major system components of this hierarchical strategy are:

1. Supercomputers
2. Parallel computers
3. Centralized general purpose computers
4. Distributed multipurpose minicomputers
5. Computing workstations and office automation support systems

Computing workstations include personal computers, scientific and engineering workstations, computer terminals, microcomputers, word processing and office automation electronic workstations, and associated software and peripheral devices costing less than $25,000 per item.

The overall Laboratory goals associated with computing workstations are:

1. To promote improved accuracy, productivity, and quality throughout the programmatic and support areas of the Laboratory by providing access to the Argonne computer network and computing tools for collecting, processing, analyzing, and transferring information more efficiently and effectively.
2. To originate and capture text and information of the Laboratory corporate database electronically.
3. To improve the communication and sharing of information among the divisions of the Laboratory.
4. To promote an environment that makes maximum use of cost-effective in-house facilities and support services (e.g., electronics repair, maintenance, and consulting) for maintaining and accommodating computing workstations.

5. To ensure that each acquisition meets the expressed need in a cost-effective manner when viewed from the perspectives of both the requesting organization and the Laboratory at large.

6. To encourage increased competition among vendors who provide computing resources to the Laboratory.

The Laboratory has developed this *Statement of Site Strategy* to be consistent with the following objectives for the acquisition and deployment of computing workstations:

1. To provide computing workstations or access to such workstations for the broad range of professional and support employees who produce or use information.

2. To provide dedicated computing workstations for users whose work requires continual access to computing resources.

3. To provide access to pools of centrally located computing workstations for occasional or intermittent users.

4. To provide a variety of recommended computing workstations, each optimized to the greatest extent possible to meet the needs of the user.

5. To provide the network capability to connect computing workstations together as well as to the other levels of the Argonne computing hierarchy.

6. To provide incentives in the form of assistance to computing workstation users to maximize compatibility and standardization among computing workstation equipment, software, and services.

7. To comply with the Argonne National Laboratory Prime Contract.

8. To comply with the Argonne National Laboratory procurement procedures.

While the primary concern of this *Statement of Site Strategy* is to ensure optimal integration of computing workstations in the hierarchy of computing that exists at Argonne National Laboratory, it also sets forth guidelines for the controlled introduction of other microprocessor technologies that become available in the computing workstation environment.

CHAPTER 2

ORGANIZATION STRUCTURE: ADP RESPONSIBILITIES

The Laboratory has established two key committees to oversee specific aspects of computing and to make recommendations to management about computer policy and use. The *Computing Policy Committee* is responsible for developing Laboratory-wide computing-related policies and for recommending those policies to the Chief Operations Officer for approval. It also establishes equitable policies for allocation of the resources of the Laboratory's shared computational facilities and addresses such issues as the standardization of computing hardware and software, new acquisitions, and maintenance. The Technical Review Committee of the Computing Policy Committee reviews system acquisition justifications to ensure that acquisitions are consistent with Laboratory directions. The Technical Review Committee also provides technical review and recommendations to the Computing Policy Committee on major hardware acquisitions. The *Administrative Data Processing Oversight Committee* (headed by the Laboratory's Chief Financial Officer) reviews, evaluates, and ranks proposals for new administrative system developments. It also recommends funding and scheduling for new developments and enhancements in existing administrative systems.

The Computing and Telecommunications Division provides a state-of-the-art computing and telecommunications foundation for Argonne National Laboratory's scientific and technical programs and administrative activities. To fulfill its mission, the Division engages in three major areas of endeavor: Scientific Research and Development, Management Information Systems, and Computing and Telecommunications Operations. Each area is headed by an Associate Division Director.

In the Scientific Research and Development area, the Computing and Telecommunications Division:

- Performs research and development in advanced scientific computing and telecommunications technologies.
- Performs applications research in supercomputing, networking, scientific visualization, parallel processing, and other areas of computer science.
- Participates in developing Laboratory initiatives and technology transfer programs in scientific computing.

In the Management Information Systems area, the Computing and Telecommunications Division:

- Provides leadership in optimizing computing and information services.
- Works with divisions, departments, programs, user groups, and Laboratory management to define needs and priorities.
- Coordinates the development of and provides maintenance for the business-related computing requirements of the Laboratory.
- Provides technical expertise and consultation in software development.

- Provides leadership in the selection and integration of administrative computing systems.

In the Computing and Telecommunications Operations area, the Computing and Telecommunications Division:

- Manages the Laboratory's central computing production systems.
- Manages the Laboratory's voice and data communications systems.
- Coordinates the development of and provides assistance for an integrated hierarchy of computing systems.
  - — Provides guidance in the use of supercomputers and large-scale central computers.
  - — Provides resources, technical guidance, and other assistance for distributed minicomputers, scientific and engineering workstations, and personal computers.
- Provides leadership in disseminating computer-related technologies throughout the Laboratory.

A fourth area, Planning, Finance, and Administration, also headed by an Associate Division Director, works with all segments of the Laboratory in developing plans, policies, and priorities for research, development, implementation, and protection of computing and telecommunications technologies.

CTD and the Electronics Department (EL) share responsibility to execute the Argonne-East computing workstation strategy. EL provides computer workstation installation, upgrades, and maintenance on request from the user organizations. At Argonne-West, onsite support organizations are similarly responsible for executing computing workstation strategy at that site.

The Procurement Department executes all computing workstation procurement requisitions in conformance with established Laboratory and DOE policies.

The Computer Users Group and its subcommittees work with CTD to identify and develop plans for meeting computing needs of the Laboratory.

The Computing Policy Committee reports directly to the Chief Operations Officer of the Laboratory. CTD works with the Chief Operations Officer and the Computing Policy Committee to implement computing policy at ANL. The Director of the Laboratory has designated the Chief Operations Officer as the Argonne National Laboratory senior management official responsible for computing activities, including computing workstation planning, acquisition, evaluation, and protection. Figure 1 shows the organization of ANL management; Figure 2 shows the organization of information technology responsibilities at the Laboratory.

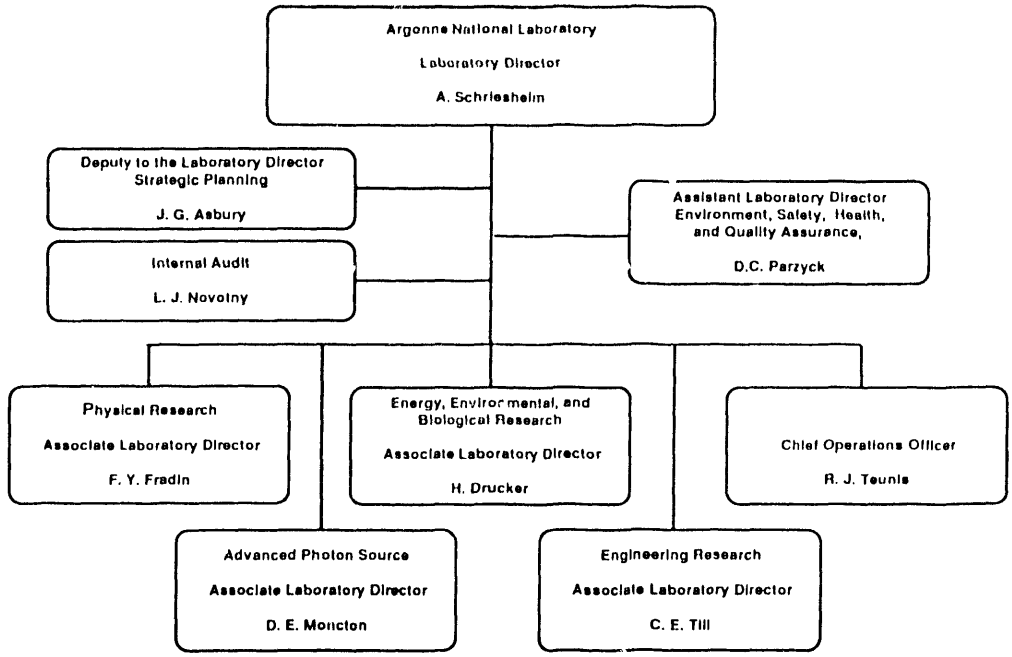

Figure 1: **ANL Management Structure**

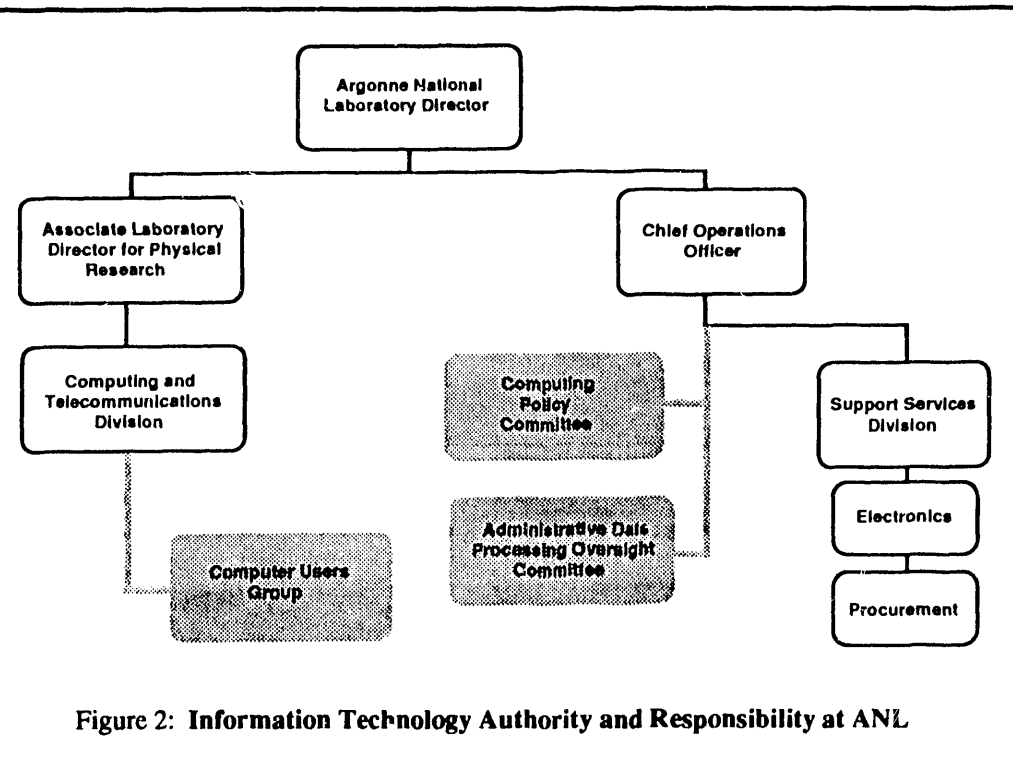

Figure 2: **Information Technology Authority and Responsibility at ANL**

CHAPTER 3

DEGREE OF CONTROL

The Argonne National Laboratory information technology resource planning and approval process covers all computing resource activities within the Laboratory, including those related to computing workstations. The overall computing workstation acquisition process is based on the annual development of the ANL *Site Response for the DOE Information Technology Resources Long-Range Plan* and the individual division, program, and department computing resource submissions to the *Site Response*. Approval of divisional, departmental, or program acquisition activities by the Computing Policy Committee is based on the quality of individual acquisition plans as well as the conformity of such plans to the stated Laboratory-wide requirements and policies on computing resource acquisition and use. Approvals and justifications for acquisition of computing equipment may include references to division and department plans. The Laboratory surveys divisions for acquisition plans in the annual *ANL Survey of Organization Plans for Word Processors, Personal Computers, Workstations, and Associated Software* (ANL/TM 459, Revision 3). The following Laboratory management and organizations have responsibility for managing various aspects of computing workstation activities:

1. Chief Operations Officer

   The Chief Operations Officer has ultimate responsibility for establishing policy and for overseeing all information technology activities, including computing workstation activities. To assist in this responsibility, the Office of Internal Audit and the Laboratory's Computer Protection Program Manager periodically assess whether computing workstation activities adhere to established Laboratory policies and procedures and advise the Chief Operations Officer accordingly.

2. Division Directors, Department Heads, and Program Managers

   The principal responsibility for planning, justification, cost benefit analysis, approval, and control of computing workstations resides in the individual divisions and departments of the Laboratory--within the guidelines and context of formalized Laboratory-wide policies and control procedures. All computing workstation procurement actions require approval by the appropriate division director, department head, or program manager.

3. Computing Policy Committee

   The Computing Policy Committee is responsible for developing Laboratory-wide computing-related policies and for recommending those policies to the Chief Operations Officer for approval. The Technical Review Committee of the Computing Policy Committee advises the Computing Policy Committee on technical aspects of the activities of divisions and departments of Argonne National Laboratory in computing resource planning, acquisition, evaluation, and protection.

4. Computer Protection Program Manager

   The Computer Protection Program Manager reviews procurement specifications for computer software valued at over $25,000; computer hardware valued at over $50,000; and all procurements for computer

hardware or software to be used in processing sensitive applications or data.[1] Reviews are for the purpose of assuring procurement specifications meet the requirements of DOE Order 1360.2A and the ANL Computer Protection Program.

5. Procurement Department

The Procurement Department executes all procurement requisitions in conformance with established Laboratory and applicable DOE policies; it reviews division, department, and project approvals for completeness and files all justifications, and it executes the procurement requisition. The Procurement Department may request review and clarification of some procurements or justifications by the Technical Review Committee of the Computing Policy Committee. The result of such review may be a request for further documentation or clarification from the originating division director or department head.

6. Electronics Department

The Electronics Department provides design, installation, and maintenance services in compliance with established Laboratory policies; it reviews all purchase requisitions for offsite maintenance services as submitted to Electronics by Procurement and determines whether in-house repair would be more cost-effective or more appropriate for other reasons such as quicker response.

7. Individual Employees

Employees acquire computing workstations, hardware, and software by developing a request and providing justification to their management for approval. The individual user is responsible for making installation and maintenance arrangements for equipment not serviced by the Electronics Department.

All new employees of ANL must sign a document confirming their understanding of and responsibility for protecting copyrighted or patented materials from misuse, and confirming their understanding of security responsibilities (see the document titled "Use of Computers at Argonne National Laboratory" in Appendix H).

All employees must comply with the requirements of the "ANL Computer Protection Plan" (available from the ANL Computer Protection Program Manager). Those who manage an application must complete the "ANL Computer Application Sensitivity Questionnaire" (also obtainable from the ANL Computer Protection Program Manager) to determine whether the application is sensitive. This "Questionnaire" is also available from the Computer Protection Program Representative for individual ANL organizations. The completed "Questionnaire" should be returned to the Computer Protection Program Representative, who will forward a copy to the ANL Computer Protection Program Manager. If the application is deemed sensitive, a determination of protection requirements will be made.

Those who manage computing workstations, hardware, or software are required to (1) protect against theft by keeping their computers in an area that is locked when the area is unattended or by securing them with a cabling device; (2) devise and follow backup procedures that protect the user from extensive loss due to user error or machine failure; (3) provide for a replacement computer in the event of a computer failure in cases where the loss of access of one or more days would be unacceptable.

[1] A computer application is sensitive if: (1) the application supports a mission-essential function where an extended interruption to services could cause a significant adverse impact to the Laboratory; or (2) unauthorized modification or disclosure of the application or data could violate statutory or regulatory restrictions, affect DOE or national interests, or cause severe legal repercussions relating to activities such as fraud, embezzlement, or breach of contract.

Those who manage a computer in a public place or a shared computer or local area network should refer to the "ANL Computer Protection Plan" for further requirements.

CHAPTER 4

PLANNING

The planning process for computing workstations at Argonne is decentralized. The individual divisions in the Laboratory identify their needs, provide justification, and perform their own reviews and productivity measurements within the general policies and guidelines issued by the Laboratory. The divisions, departments and programs of the Laboratory must analyze their individual scientific, engineering, and computing management needs; determine whether or not their applications conform to DOE computer protection guidelines; define data standards for their applications; identify areas for improvements in organizational efficiency; develop measures to determine improvements in organizational efficiency; publicize needs, applications, success and failures; and operate divisional systems. Management Information Systems annually produces *A Plan for Administrative Computing at ANL.* The document describes all planned and currently operating administrative information systems available on all levels from mainframes through workstations to personal computers. It is a tool for long-range planning for administrators and managers of computing at Argonne.

CTD and EL provide assistance for the planning activities of the divisions. The current activities of CTD and EL in the area of computing workstations are to monitor technology, to disseminate current technology information, to provide evaluation and selection assistance (hardware and software), to install and maintain systems, to assist in trouble shooting, and to recommend configurations for procurements. CTD also determines training needs, provides demonstrations on recommended computer products, develops recommended computing resource management guidelines for the Computing Policy Committee's consideration, and promotes integration of microcomputers, minicomputers, mainframes, and supercomputers. EL monitors the availability of cost-effective performance-enhancement hardware upgrades for older workstations, provides recommendations to users and upon request, modifies workstation configurations and installs upgrades as an alternative to purchasing more expensive higher performance replacement workstations. At Argonne-West, the Communications and Computer Services Section provides comparable planning and support for computing workstations.

CHAPTER 5

FUNCTIONAL NEEDS IDENTIFICATION: JUSTIFICATION AND APPROVAL PROCESS

The Laboratory has established and now maintains procedures for acquisition of computing workstations that satisfy the following objectives:

1. Evaluation of the need for computing capability that the acquisition is to satisfy.

2. Technical review to ensure that each acquisition meets the expressed need in a cost-effective manner when viewed from the perspectives of both the requesting organization and the Laboratory at large.

3. Compatibility with applicable sections of the Laboratory's long-range computing resources plan.

4. Compliance with the ANL Prime Contract.

5. Compliance with ANL and DOE Computer Protection requirements.

6. Compliance with ANL Procurement procedures.

7. Documentation at a level of detail commensurate with the complexity and magnitude of the acquisition.

8. Reduction of administrative burden and expeditious processing of all acquisition requests.

The Laboratory Director delegates signature authorization for a range of dollar amounts to specific members of management. The magnitude of the proposed expenditure generally dictates the involvement of one or more of these individuals in a given computing resource acquisition.

The review process for acquisition of computing workstation equipment and software requires contributions of time, effort, and expertise from a number of organizational entities at Argonne. The acquisition process shown in Figure 3 begins with the scientific or administrative division that is requesting equipment or software. If the acquisition cost for any single item is less than $25,000, the process culminates in a review by the responsible division director, department head, or project manager.

Users initiate the process of acquiring computing workstation hardware and software by identifying a need, developing a request, and providing justification to their division management for approval. Divisions of the Laboratory are responsible for determining the need for computing workstations and describing that need in the requisition process. The user should refer to CTD publications about recommended computing workstations. At Argonne-West, the Communications and Computer Services Section provides similar information.

Commensurate with the total estimated cost of the computing workstation requested, the requirements definition and justification should identify the specific functions and activities associated with the equipment and software: the benefits to be achieved; the provisions for protection of sensitive data or

applications; the requirements for communication with central computing resources, minicomputers, or other computing workstations; and the other requirements such as training and education. If acquisition of any single computing workstation component is greater than $1,000 and less than $25,000, the user's division completes the "Computing Workstation Equipment, Software, and Peripherals Acquisition Justification" (ANL-489) form. The user's division completes a "Purchase Requisition" (ANL-451) form,[2] attaches a completed ANL-489 form, and submits them for division director or department manager approval. Items less than $1,000 do not require submission of an ANL-489; approval of the need for such items is at the discretion of the individual Division Director or Department Manager.

Subsequent to reviewing the user request and documentation, the division director, department head, or project manager indicates his approval by signing the purchase requisition. Divisions forward any ANL-489 forms with the ANL-451 and supporting material to Procurement. Procurement reviews the completed forms according to instructions in Procurement Procedure No. 44 (see Appendix B).

[2] The Argonne-West "Purchase Requisition" form number is ANL-107-AW.

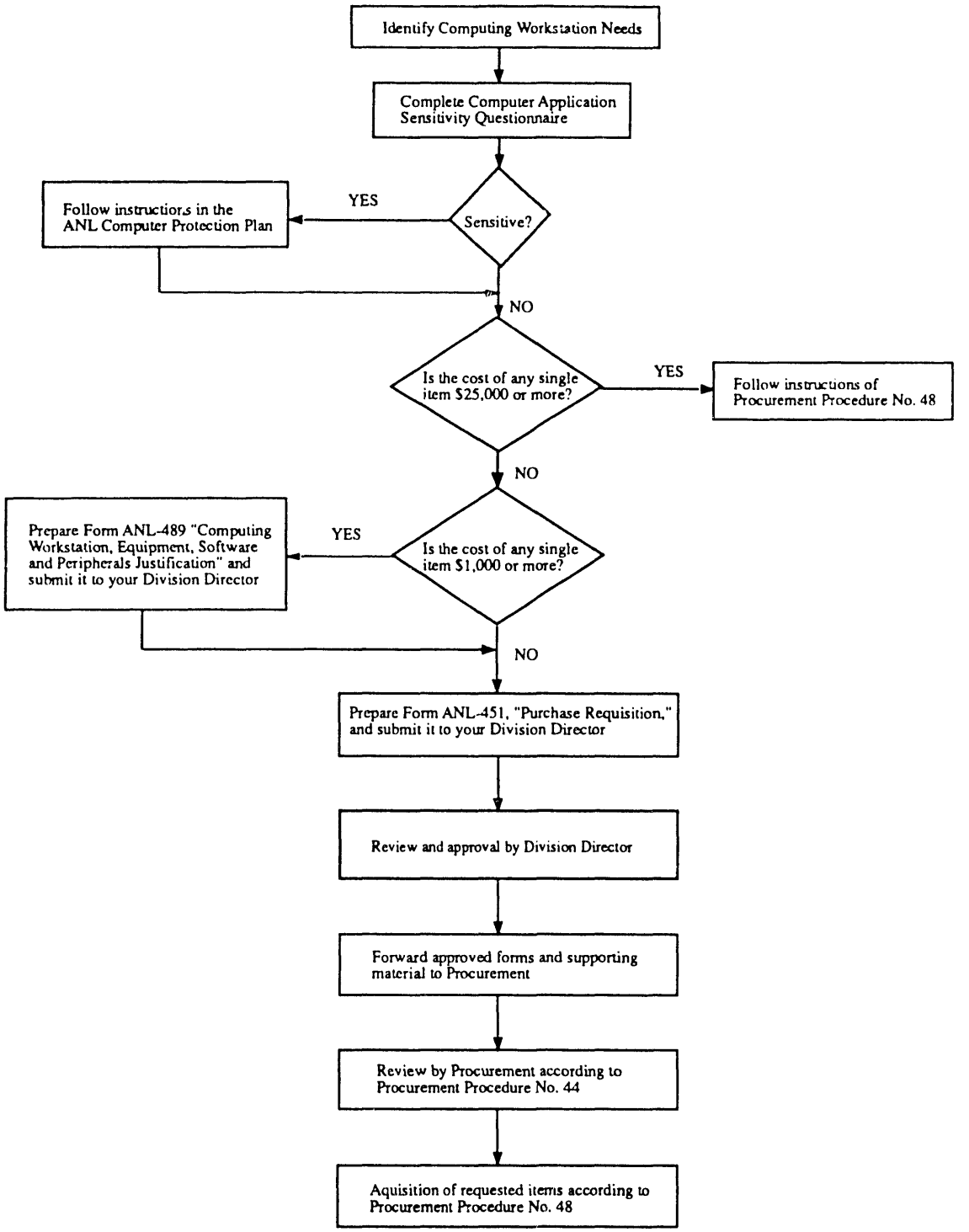

Figure 3: **Planning and Acquisition Process for Computing Workstations**

CHAPTER 6

PACE OF INTRODUCTION

To promote effective acquisitions, CTD and EL identify viable computing workstations and configurations. On the basis of equipment evaluations and early user testing, CTD and EL provide acquisition advice.

CTD establishes recommendations and standards wherever practical to promote efficiency and economies of scale. These recommendations are upgraded with emphasis on compatibility and capability. Sometimes the recommendations take the form of specific system configurations. More often, they take the form of promoting applicable industry or de facto standards for networking protocols, graphical user interfaces, graphics metafiles, laser printer page description languages, etc. The latter type of recommendation tends to have a longer-term impact. When dramatic technological or industry change occurs, old recommendations may appear obsolescent, but frequently it is not yet clear which emerging alternatives should become new recommendations. These occasions especially require CTD and EL to provide application-specific information to assist users in minimizing risks that acquired workstations may not fit well with long term directions. The vehicles for disseminating this information include the *Argonne Computing Newsletter*, the Computer Users Group, and technical memoranda. CTD provides a Workstation Evaluation and Demonstration Room (Building 221, Room A-142) containing alternate workstation configurations. This room permits Laboratory employees to develop some familiarity with these configurations prior to acquiring one.

For a summary of word processors, personal computers, workstations, and associated software, see the *Survey of ANL Organization Plans for Word Processors, Personal Computers, Workstations, and Associated Software* (ANL/TM 459, Revision 3), which is a companion document to the *Site Strategy*. The *Survey* documents the plans of each organization for scientific workstations, personal computing, local area networking, and office automation. The *Survey* identifies appropriate planners and other contact people in those organizations, and promotes the sharing of this information among those people making plans for organizations and decisions about acquiring equipment and software and implementing applications.

CHAPTER 7

PROCUREMENT: STRATEGY FOR HIGH VOLUME, MULTIPLE ACQUISITIONS

The Procurement Department coordinates purchases of computing workstations through the normal competitive bidding process. The Laboratory is taking advantage of volume purchases and contracts available from vendors and distributors for hardware and software. The Laboratory purchases Apple computer products at a discount through the University of Chicago contract with Apple Computer. Through the University of Chicago microcomputer store, ANL has arranged a site license for Mac X terminal emulation and HyperCard Developer software for Macintosh II workstations. The Laboratory has also negotiated licensing agreements (e.g., for SAS) and volume discounts (e.g., for SuperImage, SuperChart) through which users of recommended products can obtain software updates at substantially reduced costs. Through experience, the Laboratory has determined that it is not cost-effective to maintain a small inventory of personal computers or software. EL does maintain an inventory of high demand cost-effective upgrade and repair parts for existing personal computers at the Laboratory. At Argonne-West, onsite support organizations provide similar services.

CHAPTER 8

APPLICATIONS

The advances in micro chip technology are translated directly into a proliferation of distributed applications and systems for both scientific research and office automation.

In scientific computing, high powered RISC workstations provide an increase in the sophistication of simulations and the availability of scientific visualization, as well as an improvement in the programming development environment with tools for debugging and computer-aided software engineering. At the leading edge, users are beginning to implement parallel processing on a network of workstations.

Personal computers and workstations perform integral roles for the Laboratory's scientific and administrative applications. For example, IBM Personal Computers, IBM PC clones, and Apple Macintosh computers provide the platform for a number of word processing packages. Many of the personal computers are connected to local area networks to allow sharing of peripherals and data. Microsoft Word and WordPerfect on IBM Personal Computers and Microsoft Word on Apple Macintoshes are the applications used most often for preparing memos, documents, and scientific papers at ANL. The ANL Media Services Department is prepared to accept electronic input or output for typesetting a publication.

Text processing is also available on some of the distributed VAX systems. The VAX systems and the personal computers that connect to VAX or IBM host computers all participate in the Laboratory-wide electronic mail and file transfer system (see Chapter 9). Additional applications include computer graphics, computer aided engineering, spreadsheets, databases, and terminal emulation.

Single-user and local area network applications have been developed and implemented on workstations. One of the Management Information Systems applications concerning circuit data operates on a 3Com local area network and provides multiple users with updating and reporting capabilities for PBX circuit data in a shared environment using common databases. *A Plan for Administrative Computing at ANL: FY1992 through FY1994* (ANL/TM 489) lists many other administrative applications.

The Integrated Medical System and the Environment, Safety, and Health System operate in the mainframe and personal computer environments. tial data collection and most reporting are at the personal computer level while archiving, historical reporting, and data analyzing occur on the mainframe. With the mainframe as the repository for administrative data, users now have the capability, for selected databases, to extract and download the data to personal computers for use with database management systems, spreadsheets, and graphics products.

A variety of computing workstation applications serve the scientific, professional, and administrative users at Argonne. The Professional Office System (PROFS) offers electronic mail, calendar management, and document processing to approximately 100 users on the central computers. Other tools available to everyone on the central IBM computers are a text processor, a spell-checker, and an electronic mail system.

Data processing activities are merging with office functions. Authorized users have access on the central computers to Laboratory-wide databases such as a telephone directory and stores catalog. The

ANLPHONE system is an online telephone directory available to all computer users, and the Materials Catalog System provides the Laboratory with ready access to a file of stocked items and commonly used materials that are available within 24 hours. In addition, some management and information systems now combine the use of mainframe storage with the uploading and downloading of data for manipulation on a personal computer.

For a summary of workstations, see the *Survey of ANL Organization Plans for Word Processors, Personal Computers, Workstations, and Associated Software* (ANL/TM 459, REVISION 3), which is a companion document for the *Site Strategy*. The *Survey* documents each organization's plans for scientific workstations, personal computing, local area networking, and office automation. The *Survey* also identifies appropriate planners and other contact people in those organizations, and promotes the sharing of this information among those people making plans for organizations and decisions about acquiring equipment and software and implementing applications.

CHAPTER 9

TELECOMMUNICATIONS AND NETWORKING

The telecommunications and networking objectives associated with computing workstations are:

1. Computer-to-computer connections that allow file transfers at speeds approaching 100 million bits per second (MBPS) through transmission media such as fiber optic cable and cable television coaxial cable.

2. Computing workstation connections via either the PBX-based digital telecommunications system or the Laboratory-wide FDDI ring provide access to computing resources as well as communication from one computing workstation to another.

3. Intelligent gateways that provide protocol and data compatibility for interconnecting both external and internal networks of computing workstations.

4. Procurements of computing workstations by the divisions of the Laboratory that include specifications for interfacing and interconnecting computing workstations with the Laboratory-wide PBX-based digital network and the Laboratory-wide FDDI network.

5. Establishment by Laboratory divisions (within their respective planning, identification of need, and justification processes) of their own local area networks of computing workstations, provided that future plans and direction of the divisions include integration of such local area networks with the Laboratory-wide network.

CONNECTIVITY

Argonne has a large and growing network of Unix-based computers and other computers (Sun workstations, parallel processors, the Laboratory Cray, the central IBM computers, and the central VAX cluster) interconnected through the TCP/IP protocol. Users of these systems can communicate with one another by using the Simple Mail Transfer Protocol (SMTP). The Laboratory-wide TCP/IP network is also interconnected with several national and regional networks (e.g., Internet, Chicago HUB, NSFnet) and with links to other research networks). SMTP electronic mail is possible between ANL and hosts on these external networks. See Appendix C for the "ANL Network Management Policy Statement."

Argonne is a major node on the ESnet Energy Research network. Electronic mail capabilities are available for hosts connected to ESnet via a host computer at the National Energy Research Supercomputing Center at Livermore, California.

The Laboratory's Digital Equipment Corporation computers are interconnected via a Laboratory-wide DECnet. The DEC Personal Mail utility is used by these users for electronic mail communication. The ANL DECnet is, in turn, also connected to ESnet, thus enabling scientists and engineers at ANL and nationwide to communicate by using DEC mail.

Argonne has provided several bridges between the various mail systems that are currently being used. Distributed software on the DEC computers at the Laboratory provide an electronic mail bridge between the DEC mail utility and the Laboratory's NJE network. We also use the BITnet Interbit gateways to send BITnet mail to Internet hosts.

Argonne has installed IBM FAL TCP/IP for VM software on its IBM 3084 computer that runs the VM operating system. This software provides a full function interface between the Laboratory-wide TCP/IP network and VM, including an NJE-to-TCP/IP electronic mail gateway. Argonne is planning to run the Columbia Mailer, which together with FAL will act as the hub for sending mail within the Laboratory and as an interface to several external networks, including BITnet, NSFnet, and Internet. The implementation of the Columbia Mailer will eliminate the need to have host tables on distributed Argonne systems. An ongoing activity will provide X.400 and X.500 name service for the DEC electronic mail network.

LABORATORY-WIDE NETWORK STRATEGY

The PBX-Based Digital Telecommunications System provides a Laboratory-wide local area network capability (LANmark). A major local network strategy is to provide a Laboratory-wide Ethernet that allows simultaneous connectivity to a small, select set of network protocols: DECnet, TCP/IP, XNS, LAT, and Appletalk. The programmatic divisions at Argonne are heavily DEC VAX-based with DECnet and LAT protocols. The fastest growing trend in networking protocols is TCP/IP, allowing scientists to communicate from personal computers and workstations to the Cray X-MP supercomputer, to the MCS Advanced Computing Research Facility, and to other TCP/IP hosts on the Laboratory-wide Ethernet. Fourteen 3Com EtherSeries networks are in use at Argonne running the XNS protocol. Several DECnet LANS have implemented Pathworks for IBM PCs and Macintosh. Novell local area networks, which use the IPX protocol, have also begun to be installed.

Efforts are under way to connect these PC LANS to the Lab-wide Ethernet and introduce them to a Simple Mail Transfer Protocol (SMTP) E- mail system.

The Argonne Fiber Distributed Data Interface (FDDI) project is an important step in positioning ANL to take advantage of high-speed fiber-optic networking. Interfaces for Sun and Silicon Graphics workstations have been tested; similar tests are planned for IBM and DEC interfaces, as well. Initial tests show that network file transfers run four to five times as fast over FDDI as over Ethernet. Some scientific visualization programs have been run over FDDI and have shown similar performance results.

In the near future, FDDI will become the primary path for TCP/IP users to access the Cray X-MP/18. Most users attached to the Laboratory- wide Ethernet through LANmark should notice no performance or functional changes. CTD will make this change to provide faster access to the Cray via divisional FDDI connections. CTD and the Environmental Assessment and Information Sciences Division are obtaining connections of this type. CTD has connected a Cisco multiprotocol router between the CTD FDDI ring and the Laboratory-wide Ethernet. Also, a Network System Corporation FDDI interface connects the Cray X-MP/18 to the CTD FDDI ring. The Sun TCP/IP interface to the Cray will remain in place and serve as a back-up path.

The implementation of a Laboratory-wide FDDI network is also in progress. CTD has developed specifications and a charging method, so that divisions can order routers and have CTD install, configure, and manage them. A fiber-optic cable now connects the offsite Building 900 networks to the Laboratory-wide FDDI network. Other divisions have indicated an interest in connecting local area networks to the FDDI backbone network. CTD has submitted a proposal to request funding to interconnect twenty-five buildings with fiber-optic cable. CTD has expanded its proposal to permit a distributed video teleconferencing service.

SECURITY

The Laboratory-wide Ethernet provides point-to-point transmission of packets and, as such, is an acceptable medium for the transmission of sensitive (but not classified) information. Access to the Laboratory-wide FDDI ring is controlled by secured routers; thus the Laboratory-wide FDDI ring is also an acceptable medium for use in transporting sensitive (but not classified) information.

Those who wish to use divisional Ethernets or FDDI rings must consider the risks of having that information intercepted by unauthorized persons and write a protection plan that ameliorates those risks.

CHAPTER 10

DATA ADMINISTRATION

Data administration encompasses managing the information, making it available to those who need it, controlling the access to it so that unauthorized persons cannot access data for which they have no authorization, providing a back-up strategy, and assuring compliance with ANL and DOE Computer Protection requirements. The Laboratory-wide administrative databases are comprised of personnel, financial, and property data and are accessible by Laboratory management and other persons authorized to use administrative data. Access is approved by the primary administrative organization (e.g., HR, OCF) and implemented by CTD.

Currently, the Human Resource System (HRS) provides a series of standard reports that meet many of the personnel information needs of division and program management. Users can query the HRS database directly in CMS. Only specific users who justify their requests can obtain permission to extract and download data from sensitive Laboratory-wide databases (e.g., HRS). Typically, the user contacts CTD and fills out a form requesting HRS access to a specific Laboratory-wide database. Overall control of access to Laboratory-wide databases is the responsibility of the "owner" of the database, who is usually one of the division directors or department heads within Operations. In the case of HRS, the Director of Human Resources authorizes access to the requested items only and not to the entire database.

The Integrated Financial System (IFS) is considered a non-sensitive system. Currently, selected computer users with CICS/MVS accounts may access IFS data. Access to Integrated Payroll System data and to Integrated Personnel Management System data is restricted to assigned Management Information Systems analysts and to authorized computer users in Human Resources, in the Office of the Chief Financial Officer, and (at Argonne-West) in Administrative Services.

Each division has a property representative with responsibility for the accuracy of property information. The Property System is available in CMS and is open to all property representatives at the Laboratory. This system uses the INQUIRE database for its data management.

CTD is responsible for the administration of the PROFS system, including access and, update controls for calendars, audit trails, and use. A PROFS account is available to anyone with a CMS account.

The administrator of a division's local area network is also responsible for the administration of data for that network.

The user of information developed or maintained on a computing workstation is responsible for completing a "Computer Application Sensitivity Questionnaire" for the application. If the application is determined to be sensitive, the user is responsible for completing the "Sensitive Computer System Checklist" and for writing a risk assessment and protection plan for the system. The risk assessment must be approved by the divisional Computer Protection Program Representative.

CHAPTER 11

SOFTWARE

The Laboratory is committed to purchasing software when possible rather than to developing code internally. To reduce maintenance costs and to allow smoother transition to product upgrading, the Laboratory ordinarily follows a policy of not modifying standard software.

PROCESSING SOFTWARE REGISTRATION AND LICENSE AGREEMENTS

Most personal computer software today comes with so-called implicit license agreements. Typically, there is a warning not to open the package unless the user agrees to the license conditions. This warning may state that simply opening the package commits the user to the license conditions. In fact, these statements have no legal basis, and simply unwrapping the software will not commit the user or the Laboratory to the license agreement. However, such personal computer software packages usually contain a registration card that, when completed, signed, and returned to the vendor, entitles the user to software updates, hot line assistance, newsletters, etc. Signing the registration card may commit the user to the software license terms and conditions, some of which may be unacceptable to the Laboratory. Only the Procurement Department should commit the Laboratory to software license agreements with vendors.

Argonne therefore requires that employees submit all such license agreements (unsigned) to the Procurement Department for review. Procurement in turn submits these agreements to ANL Legal for review. The specific procedure for handling these personal computer software registration cards is:

1. The user fills in the requested information (e.g., name, address, and serial number) on the card but does not sign it.

2. The user forwards the card to Procurement in Building 201.

3. Procurement (with the assistance of ANL Legal) reviews and revises the terms and conditions, if necessary, and mails the registration card to the vendor.

COMPLYING WITH SOFTWARE LICENSE AGREEMENTS

A Laboratory memorandum dated October 3, 1991, to all employees outlines user responsibilities when employees use the proprietary computer programs (see Appendix G). In particular, employees must not make unauthorized copies of such programs either for their own use or for the use of others.

See also "Complying with Software Licenses" in Chapter 15.

DISPOSING OF OBSOLETE SOFTWARE

Eventually, personal computer software becomes obsolete to the point where it should never be needed or used again, because of many better, more up-to-date alternatives.

The Laboratory recommends that users having obsolete software do one of the following:

- Keep floppy disks containing obsolete software on file within the organization.
- Reformat the floppy disks and reuse them for other purposes.
- Discard the obsolete disks.

When floppy disks containing such software are discarded or reused, records must by kept on file by the division noting the method and date of disposal. This record should be attached to or (in the case of electronic record keeping) associated with the purchase order.

CHAPTER 12

STANDARDS

The development of standards is a dynamic process that must include consideration of the functional needs and requirements of the user community, the existing investment in working applications, and the changing computing workstation marketplace. Clearly, no single combination of computing workstation equipment and software can satisfy all the different and changing needs of the personnel of the Laboratory who require the use of a computing workstation now or in the future. Consequently, while it is critical to promote integration standards for networking, printing, and data exchange, it is not always practical to require a standard product for a given application.

In the area of scientific computing and in the context of scientific workstations, the standard user environment is commonly assumed to involve a Unix operating system, TCP/IP networking, an X Windows graphics environment, and the Network File System for remote data storage. In a heterogenous vendor environment, however, the reality is that Unix is sufficiently standardized to enable users familiar with one vendor's Unix implementation to be quite productive with another vendor's implementation despite implementation differences. Still, it is true that graphics programs written in high-level graphics languages for one vendor's platform are typically not able to run on other, different platforms. The X Windows graphics environment does provide a great deal of standardization, albeit with tedious low-level programming; in fact, X Windows enables graphics applications to display images on virtually any Unix workstation with X Windows. CTD encourages the use of X Windows on central and distributed computers alike.

CTD is working with and assisting the current and anticipated computing workstation users in identifying the most cost-effective mix or combination of equipment and software to meet users needs. Currently, CTD promotes equipment and software selections that make use of Ethernet standards (TCP/IP, Decnet), PostScript page description language, the X Windows graphics system, the CGM graphics metafile standard, AppleTalk, PC DOS, MS Windows, and SMTP (Simple Mail Transfer Protocol) to connect to Laboratory-wide electronic mail.

Personal-computer-based and scientific-workstation-based drafting systems that use AutoCad software have become prevalent at the Laboratory. Becuse of its low cost, its good performance, and the considerable ANL operating experience with it, the Computing Policy Committee has recommended AutoCad for any future acquisitions of personal computer-based drafting systems. Further, the Engineering Physics Division provides a conversion program permitting Autocad users to interchange drawings with the Laboratory's more powerful Intergraph system.

Additionally, the Computing Policy Committee has recommended that computing workstations acquired for interactive engineering, design, or drafting must be compatible with the existing Intergraph-based infrastructure at the Laboratory. Also, the CAE subcommittee has recommended that any personal-computer-based drafting systems or software be compatible with AutoCad for transferring graphics to the Laboratory's Intergraph system.

CHAPTER 13

SUPPORT STRUCTURES

Assistance is available for selected products, needs analysis, product selection, user education, procurement, and maintenance. CTD and EL provide assistance to users in selecting and configuring computing workstation equipment and software. Users from CTD, EL, and other divisions participate in the evaluation process. User groups are active in providing input into planning, product evaluation, and other actions related to computing workstations. EL can also provide information on obtaining maintenance and on the reliability of particular computer and peripheral equipment.

CTD and EL evaluate computing workstations, software, and peripheral devices. EL and CTD also disseminate information on recommended products to the Laboratory and provide user assistance. In addition, CTD ensures compatibility and integration for its recommended hardware and equipment.

CTD configures and installs computing workstation systems and local area networks as specified by the overall Laboratory Computing Strategy and recommended by CTD.

EL designs, configures, and installs computing workstations and network systems from a variety of vendors and can assist users on deciding which configuration best meets their needs. EL maintains an inventory of repair parts, loaner systems, system software, and peripherals. EL provides repair and maintenance services either on an as needed basis or by providing fixed cost maintenance contracts. EL also provides system upgrade services as a cost saving alternative to the replacement of existing workstations with more expensive new workstations. The user is responsible for making servicing arrangements with EL or the appropriate vendor.

The Procurement Department contracts for the lowest price consistent with technical and delivery requirements. Procurement has contracted block purchases of certain recommended products. Procurement forwards purchase requisitions for all repair work to EL for determination of whether the repairs should be performed in-house or procured from outside sources.

At Argonne-West, onsite support organizations provide similar assistance and support activities.

CHAPTER 14

TRAINING AND EDUCATION

The Laboratory addresses computing workstation training and educational requirements in a variety of ways. CTD uses word-processing education available from word-processing vendors in conjunction with educational courses developed in-house. Training diskettes and tutorials are available for personal computer education. Some assistance in how to use the personal computer is available for new users. CTD offers instruction on data communication and hard-disk management. CTD also provides assistance in the formation of user groups for the Apple Macintosh computers and Local Area Networks. Information exchange is available for users groups and other participants.

Varying levels of computer familiarity among users indicate that the Laboratory needs a more extensive educational program. CTD currently provides a variety of training and educational opportunities for computing workstation users. In response to feedback from the various computing user groups of the Laboratory, CTD has coordinated additional training and educational courses and seminars focusing on computing workstations. Human Resources coordinates several personal computer software classes that are provided through the local DOE Computer Resource Center. Some of the available classes introduce DOS, personal computers, DBase III, DBase IV, Lotus 1-2-3, Harvard Graphics, VideoShow, and Word Perfect.

A Personal-Computer Local-Area-Network Administrators Group meets periodically to discuss current issues, and an Apple Macintosh Users Group has been thriving at ANL for many years. CTD occasionally makes presentations about services and policies for such user groups. Minutes of these user group meetings are published in the *Argonne Computing Newsletter*.

CHAPTER 15

SECURITY

The Laboratory has instituted a computer protection policy in compliance with DOE Order 1360.2A (see Appendix D). This policy provides guidance for protection of Laboratory computer systems and unclassified but sensitive applications and data. The Laboratory also has a "Computer Protection Plan" (available from the Computer Protection Program Manager) that states the protection requirements for non-sensitive computers and provides a set of requirements that individual protection plans for sensitive computers must meet. *Guide to Computer Protection at ANL* (ANL/TM 413) defines the protection procedures.

The Laboratory has also instituted a Computer Security Education and Awareness Program. Each employee who manages, operates, develops, or maintains a computer or computer application must receive computer security education and awareness training annually. This education and training includes information on the responsibilities of computer users and is provided by The divisional Computer Protection Program Representatives.

Computer incidents must be reported to the appropriate authorities as requested by the "ANL Computer Security Incident Reporting Procedure" (see Appendix E).

Every ANL organization that uses computers appoints a computer protection program representative. This representative is responsible for ensuring protection policy compliance for divisional applications and computers. The representative is also responsible for approving divisional protection plans and risk assessments and for providing computer security education and awareness training for division personnel. The representative also acts as a divisional contact point for relaying timely security information to those within the division who need the information. In addition, the representative answers questions concerning individual responsibilities for computer protection.

MANAGING SENSITIVE APPLICATIONS

Laboratory policy requires that managers of all computer applications determine the sensitivity of their applications by completing a "Computer Application Sensitivity Questionnaire" for each application. This requirement is not only for computer applications on the central and distributed divisional computers but for those on personal computers and word processors as well. The questionnaires should be returned to the Computer Protection Program Representative, who reviews them and forwards them to the ANL Computer Protection Program Manager. Managers must prepare a protection plan for every application deemed to be sensitive.

Each protection plan must meet the requirements of one of four summary protection plans prepared by the Laboratory in compliance with the Computer Security and Privacy Act of 1987. Those who have questions concerning this area should address them to their divisional computer protection program representative or call the ANL Computer Protection Program Manager at extension 2-7440.

The Laboratory's protection requirements are:

- Offices and other areas containing computing workstations must be locked when they are unattended. If the area cannot be locked, the computing workstation must be securely fastened to a desk or table with a commercially available locking device.
- Diskettes containing sensitive applications or data must be stored in locked areas, desks, or filing cabinets.
- Software data stored on backup disks that are accessible to unauthorized users must be password-protected. Similarly, backups made of sensitive data must be protected.
- Sensitive data existing on shared disks accessed by computers on local area networks must have password protection, and sensitive data printed on printers at multi-user stations must be protected against disclosure.

Those planning to use local area networks for transmitting sensitive information must include in their risk assessments the risk that unauthorized persons could access the information flowing through the network and address those risks in their protection plans.

Individual situations may call for additional protection mechanisms. Those who manage a sensitive application must assess the vulnerabilities and risks and determine whether additional protection is necessary.

COMPLYING WITH SOFTWARE LICENSES

Laboratory and DOE policy prohibits the unauthorized duplication and use of computer software. Software piracy or unauthorized duplication is a crime. Unauthorized duplication and use of computer software violates the U.S. Copyright Law and unfairly deprives software developers of revenue for their work.

Unless otherwise specified in a license agreement, the funds used to purchase a software product represent a license fee for the use of one copy of the software product. Should the software be reproduced or duplicated without authorization, then the U.S. Copyright Law has been violated, making the infringement a federal offense. When software is used on a local area network service, all those who have access to that software on the service must be licensed to use that software. Unless the license is specifically written to include network use, individual licenses must be purchased for every person able to access the software on the service. Civil damages for unauthorized software copying can be as much as $50,000, and additional criminal penalties such as fines and imprisonment can be imposed.

Should any situation arise as a result of unauthorized use of computer software, the person responsible will be held liable for any compensation required as a result of legal action and will also be subject to disciplinary action by the Laboratory.

All new employees of ANL must sign a document confirming their understanding of and responsibility for protecting copyrighted or patented material from misuse, and confirming their understanding of security responsibilities.

ANTI-VIRUS ACTIVITIES

To combat the threat to ANL of viruses that can attack computers that use the MS-DOS operating system, CTD has obtained the Clean-up Version V77 and Viruscan V77 programs. Previously, CTD had purchased a license for 100 copies and has already distributed copies to Argonne's IBM personal computer virus fighting team members. The Clean-up program attempts to remove viral infections from files that cannot be restored from a back-up disk. Version 77 can disinfect over 481 different types of viral infections.

CTD has established teams for each major operating system at the Laboratory to prevent a successful attack or to mitigate the effects of such an attack. Team membership includes system experts both within and outside CTD. Users must report all viruses, worms, attempted system break-ins, or other incidents that represent a threat to ANL computer systems to the Computer Protection Program Manager.

REMOTE LOGIN SECURITY RULES

Any data accessible by remote login is only as secure as data on the least secure computer in the chain. Remote logins propagate any poor security practices from local computers to the mainframe. To ensure individual accountability on local systems, system managers must take care in setting system parameters and in establishing secure practices to prevent access to the local system by unauthorized persons. These practices include requiring all system users to practice good password management that ensures individual accountability. Any time that accountability on local systems is compromised and the local system users avail themselves of remote logins to mainframe computers, the mainframe acccunts will also be compromised. All ANL and DOE computer security policies require users with computing accounts to maintain individual accountability; failure to do so (e.g., by sharing login passwords with others) is considered a computer security incident and is reportable to Laboratory management.

For example, Cray UNICOS, like most Unix systems, provides easy access from a remote system, such as a workstation. The capabilities include the **`rlogin`** and **`rsh`** commands. By having an ".rhost" file in the home directory on the Cray that lists the user's workstation name and userid, the user can login *without providing the Cray password* by entering the **`rlogin`** command or can execute commands *without providing the Cray password* by entering the **`rsh`** command. The exploitation of the ".rhost" capabilities involves a security risk. The Cray account is only as secure as the workstation account. If other users can use the workstation account, they can also **`rlogin`** to the Cray. If users exploit the ".rhost" capability across many nodes, the security of all user accounts is only as good as the weakest security on any node. Several reported instances of stealing password files and guessing passwords have stemmed from indiscriminate use of ".rhost" files. Some Argonne users have been affected.

Although the use of ".rhost" files on the Cray is allowed, each user must weigh the risks involved. CTD recommends that users create ".rhost" entries only for their everyday workstations. The security of the workstations should be reviewed with the system manager. All ".rhost" files should be reviewed on a regular basis, and unused entries should be removed. These ".rhost" files should never be used from a system where the system manager is unknown or the security procedures are unfamiliar. CTD requires that users with sensitive applications on the Cray not create ".rhost" entries for hosts that have insufficient protection for these sensitive applications.

CTD recommends that computer users strengthen the computer protection program by:

- Choosing good user verification (logon) passwords.
- Changing passwords at least once every six months.
- Not sharing passwords with others.

A good password:

- Is not in the dictionary.
- Is not easily associated with the user or any information about the user.
- Is not the name of a well-known real or fictional character.
- Is a combination of alphabetical and special characters or numbers.
- Is easily remembered.

Recommended choices for passwords include two short words joined by one or more special characters or numbers.

The Computer Protection Program Manager receives all Computer Incident Advisory Capability (CIAC) notices (issued by DOE) and distributes these notices of computer vulnerabilities to all persons whose names appear on the security bulletin mailing list. All system managers thus receive these notices from the Computer Protection Program Manager. System managers must consider all such notices carefully and implement any additional security measures appropriate for a particular system and its environment.

CHAPTER 16

TECHNOLOGY ASSESSMENT

Testing of new computing workstation equipment and software products is an ongoing process that involves expertise from CTD, Mathematics and Computer Science, EL, and various other Laboratory organizations. These tests are normally to determine functionality, ease of use, compatability with onsite and national networks, ease of maintenance, future growth, and cost.

No organization has sufficient effort available to assess all emerging workstation technologies. ANL must use its available testing resources selectively to assess the emerging technologies most relevant to the ANL computing environment. For example, technologies requiring particular attention at least for the next few years include networking standards (OSI, GOSIP, FDDI, PC Lans), advanced RISC workstations, advanced graphics workstations, standards for transmission of video, distributed applications designs based on the client-server model, optical storage, and standards (X11R5, Phigs, PEX, etc.) for the transmission and display of three-dimensional graphics objects.

CHAPTER 17

EVALUATION

Each ANL division is interested in acquiring hardware and software capabilities to meet specific programmatic research objectives. To that end, each division invests significantly in evaluating capabilities for its particular application needs. Where there are broad areas of interest and applicability, CTD and EL conduct evaluations, benchmarks, and tests to assist divisions in making acquisition decisions. Recommendations are documented in the *Argonne Computing Newsletter* when appropriate. Otherwise, information is shared among organizations in the course of day-to-day interactions.

Overall increases in efficiency and any other effects on Laboratory work that accrue from the acquisition and installation of computing workstations must be reviewed by the respective division directors, program managers, and department heads in conjunction with the ongoing review and approval of individual computing workstation requests and justifications.

CTD performs an annual survey of installed word processors, personal computers, computing workstations, and associated software to identify trends in ANL computing, to identify appropriate contacts for each division, and to provide a basis for planning by support organizations. The results of the 1991 survey appear in the *Survey of ANL Organization Plans for Word Processors, Personal Computers, Workstations, and Associated Software* (ANL/TM 459, Revision 3). CTD distributes the *Survey* to division directors and department heads; it is also available at the Document Distribution Counter (Building 221, Room A-134) or through the mail (by calling extension 2-5405 and ordering a copy).

APPENDIX A

COMPUTING WORKSTATION COMPONENT ACQUISITION POLICY

1. PURPOSE

   This policy provides guidance for the justification and acquisition of computing workstations at Argonne.

2. SCOPE

   This policy covers personal computers, microcomputers, computer terminals, combined voice/data terminals, word processing and office automation electronic workstations, and associated software and peripheral devices costing less than $25,000 per item.

3. POLICY

   It is Laboratory policy (1) to actively promote the installation and use of computing workstations to improve productivity and communications for both programmatic and support personnel, (2) to ensure that computing workstation acquisitions meet the expressed need in a cost-effective manner, and (3) to document the acquisitions of computing workstations in accordance with DOE Order 1360.1A (5/30/86) and the ANL Statement of Site Strategy for computing workstations.

4. GOALS

   a. To promote improved accuracy, productivity, and quality throughout the programmatic and support areas of the Laboratory by providing access to the Argonne computer network and computing tools for collecting, processing, analyzing, and transferring information more efficiently and effectively.

   b. To ensure that each acquisition meets the expressed need in a cost-effective manner when viewed from the perspectives of both the requesting organization and the Laboratory at large.

   c. To promote an environment in which maximum use is made of cost-effective in-house facilities and support services (e.g., electronics repair, maintenance, and consulting for computing workstations).

   d. To provide a variety of recommended computing workstations with each optimized to the greatest extent possible to meet the needs of the user.

   e. To provide incentives in the form of support and assistance to computing workstation users to maximize compatibility and standardization among computing workstation equipment, software, and services.

   f. To comply with the Argonne National Laboratory Prime Contract.

   g. To comply with the Argonne National Laboratory procurement procedures.

5. RESPONSIBILITIES

a. The Chief Operations Officer has ultimate responsibility for establishing policy and for overseeing all ADP activities, including computing workstation activities.

b. The Office of Internal Audit and the Laboratory's Computer Protection Program Manager will periodically assess whether computing workstation activities adhere to established Laboratory policies and procedures and will advise the Chief Operations Officer accordingly.

c. The Computing Policy Committee is responsible for development of Laboratory-wide computing-related policies and for recommending those policies to the Chief Operations Officer for approval. The Technical Review Committee of the Computing Policy Committee has been established to assist Divisions and Departments of Argonne National Laboratory in ADP planning, acquisition, evaluation, and protection.

d. Employees acquire computing workstations, hardware, and software by developing a request and providing justification to their management for approval.

e. Division Directors, Department Managers, and Project Managers are responsible for planning for and approving workstation justifications, and controlling computing workstations for their organizations.

f. The Procurement Department executes all procurement requisitions in conformance with established Laboratory policies. It reviews Division/Department/Project approvals for completeness, files any supporting justifications, and executes the procurement requisition.

g. CTD implements computing policy formulated by the Argonne Computing Policy Committee, for which it drafts plans and prepares recommendations; it works with other Argonne divisions and programs, user groups, and Laboratory management to determine specific needs and priorities. CTD evaluates computing workstations, software, and peripheral devices and makes recommendations to the Chief Operations Officer as to which computing workstations, software, and peripheral devices are to be recommended for use at the Laboratory. The CTD also disseminates information on recommended products to the Laboratory and provides user assistance.

h. The user is responsible for making service arrangements with the Electronics Department. Prior to issuance of a purchase order, Electronics will review all purchase requisitions for maintenance by offsite vendors and determine whether in-house maintenance and repairs would be more appropriate and cost-effective.

6. DEFINITIONS

a. Computing workstation components include personal computers, computer terminals, microcomputers, combined voice and data terminals, word processing, and office automation electronic workstations.

b. A personal computer is a general purpose microprocessor-based computer system.

c. "Microcomputer" is a term DOE uses to refer to a personal desktop computer.

d. A computer terminal is a workstation used to communicate with a host computer; the application software is resident on the host computer.

e. Word processing and office automation workstations are computing workstations designed primarily for secretarial and clerical activities to perform word processing and related office functions.

f. Software consists of programs that computing workstation users access to do their work.

g. Peripheral devices are items such as modems, printers, and plotters connected to computing workstations.

7. IMPLEMENTATION

The user identifies the need for a workstation. The user may obtain assistance from CTD in defining requirements, visit the Workstation Evaluation and Demonstration Room to compare recommended workstation alternatives, and refer to Computing and Telecommunications publications about recommended computing workstations. For any single item costing more than $1,000 but less than $25,000, the user's division completes the "Computing Workstation Equipment, Software, and Peripherals Acquisition Justification" (ANL-489) form. The user's division completes a "Purchase Requisition" (ANL-451) form, attaches a completed ANL-489 form (where required), and submits them for Division Director or Department Manager approval. Divisions forward any ANL-489 forms with ANL-451 forms and supporting material to Procurement. Procurement reviews the completed forms according to instructions in Procurement Procedure No. 44.

APPENDIX B

PROCUREMENT PROCEDURE NO. 44: COMPUTING WORKSTATION COMPONENTS

1. GENERAL

The purpose of this procedure is to define the authority and responsibility for control, approval, and management of requisitions for personal computer(s), workstation(s), and components from Stores inventory and from outside suppliers.

2. DEFINITION

COMPUTING WORKSTATIONS are defined as personal desktop computers, computer terminals, microcomputers, combined voice/data terminals, word processing and office automation electronic workstations, and associated software and peripheral devices of less than $25,000 per item.

3. RESPONSIBILITY

a. REQUESTING DIVISION(s), DEPARTMENT(s), and PROJECT MANAGEMENT(s)

Are responsible for issuing the request and providing justifications for computing workstation components. See *ANL Policy Manual*, "General Administrative Matters," Part XXI.

b. PROCUREMENT DEPARTMENT (PRO)

Is responsible for reviewing the necessary requisition forms for completeness, and procurement will only accept requisitions that are adequately and properly justified.

4. PROCEDURE

REQUESTING DIVISION:

a. Prepares Forms ANL-451 and ANL-489 for materials requested from outside suppliers. After proper execution of forms, forwards them to the Procurement Department (PRO) for processing. Items valued less than $1,000 do not require submission of an ANL-489 form.

b. Completes the "ANL Computer Application Sensitivity Questionnaire" for workstations and computer applications. For sensitive workstations or applications, the Division completes a risk assessment and a protection plan, then completes the "Sensitive Computer System (or Application) Checklist" and sends it with a request to approve the procurement to the ANL Computer Protection Program Manager.

c. Obtains a memorandum of approval from the ANL Computer Site Security Manager for workstations and computer applications that process classified information.

d. Prepares and submits the "Government Open Systems Interconnect Profile" (GOSIP) questionnaire and statement of compliance/applicability.

PROCUREMENT:

a. Reviews the request form to determine whether the request is consistent with the ANL Statement of Strategy, and if so, enters the Form ANL-451 into the AMPS system.

   In the event PRO requires additional information to ensure that the justification is adequate, contacts the requesting division or the Technical Advisory Committee of the Computing Policy Committee. PRO will retain the Form ANL-489 for permanent file. Purchase requisitions (Form ANL-451) for materials from an outside supplier will be processed through the normal procurement procedure.

b. Verifies that a letter of approval from the ANL Computer Protection Program Manager is filed with the request if the workstation or application is sensitive as identified on Form-489.

c. Verifies that a letter of approval from the ANL Computer Site Security Manager is filed with the request if the workstation or application is to be used to process classified information.

APPENDIX C

ANL NETWORK MANAGEMENT POLICY STATEMENT

The installation of the ANL Lab-wide Ethernet has greatly increased Local Area Networking capabilities at ANL-East. However, as more and more Divisions and Projects make use of the network for routine work, the potential for inadvertent disruption of the network also increases. To decrease the possibility of temporary disruption to networking services and to provide for the orderly growth of the network, we recommend the following:

1. Establish an ANL Network Managers working group.

   a. Membership

      1) Chairperson to be selected by the CPC Networks Subcommittee with concurrence from the CPC.

      2) A liaison to the CTD Networks Section who would serve as an ex-officio member in addition to the CTD working group representative.

      3) One representative from each cost center or other functional entity presently using the Lab-wide Ethernet, including appropriate representatives from ANL-W. To this end, a memorandum from the Laboratory Chief Operations Officer should be sent to all Division Directors, Project Managers, and Department Heads requiring the appointment of a *technically knowledgable* individual to serve as a member of the working group for all organizations presently using or planning to use ANL network services. It should be stipulated that the individual chosen be given *complete authority* within that organization to implement the policies and procedures of the Network Managers working group.

         In some cases, it may be helpful to build a hierarchical committee structure within each organization to assist the working group representative. The next lower level would typically consist of technical sub-network managers, such as those responsible for Sun workstation, PC, and DECnet networks. The lowest level would normally consist of workstation end-users and managers of small systems.

   b. Function

      1) Coordinate implementation of CPC networking policies, disseminate networking information throughout their organizations, and enforce agreed upon procedures for connecting equipment and software systems that may affect the operation of the network.

      2) Interact with CTD personnel to help keep the network functioning smoothly and to address malfunctions in its operation.

      3) Assist Computer Protection Representatives in responding to network threats such as viruses and intrusions.

4) Meet as required by the designated chairman (or as the group otherwise decides) and report to the CPC Networks Subcommittee as warranted.

2. The Network Managers working group representatives would have primary responsibility for approving standard connection requests in a timely fashion. The CTD Networks Section liaison would have responsibility for approving non-standard network connection requests. Those connections requiring special consideration (see below) would be permitted only with the concurrence of an ad-hoc advisory committee to the Networks Working group and would consist of a small number of individuals technically expert in the various protocols, operating systems, and hardware in use on the network.

3. The Network Managers working group would assist in the specifying and updating of a network equipment database, which at a minimum would contain the following information for each piece of equipment capable of transmitting data on the Lab-wide Ethernet: system type and location, network software and version, network hardware, network address (physical Ethernet and software-specific), system contact, location and phone, and date of installation (or date to be installed).

4. Connection Requirements

   a. Network hardware and software would be categorized by the CTD Networks Section as follows:

      1) *Preapproved* -- all equipment and software presently being successfully used on the network.

      2) *Tentatively approved* -- new, untried versions of low-risk equipment and software. (These would be recategorized after completion of a successful probationary period.)

      3) *Not-yet approved* -- all other new, untested equipment and software. These would also be recategorized.

      4) *Disapproved* -- equipment and/or software found to be incompatible with proper operation of the network and excluded from network participation.

   b. Each of the above would carry separate requirements as defined below:

      1) All categories of equipment require *prior approval* of each organization's Network Manager and registration in the network database.

      2) Addition of preapproved equipment carries no further requirements other than adherence to policies governing the selection of software/hardware parameters for that equipment.

      3) Addition of tentatively and not-yet approved equipment requires following an approved test procedure and prior notification to working group representatives of testing plans. It is recommended that there be a 1-2 day probationary period during which any Network Manager may request the removal of the equipment should network disruptions occur. For tentatively approved equipment and software, on-network testing during non-prime working hours might suffice as a testing plan. Prior approval by the CTD Networks liaison is required.

      4) Addition of not yet approved equipment requires prior approval by the network ad-hoc advisory committee of the testing plan for the new equipment and final approval by the Networks liaison. Equipment/software causing network disruption will be categorized as *disapproved.*

      5) The committee recognizes that the attachment of even approved equipment can be disruptive to the network if software parameters and/or hardware switches are not appropriately set. It is the responsibility of the Cost Center (CC) Networks Manager to assure that his/her organization has appropriate controls and procedures for obtaining, setting up, or changing systems parameters as needed.

6) Before implementing new local area network technology that is significantly different from existing ANL networking directions, the Cost Center Networks Manager must inform the Network Managers Working Group of plans for review and discussion.

APPENDIX D

ANL COMPUTER PROTECTION POLICY

1. PURPOSE

This policy exists to provide guidance for the protection of Laboratory unclassified computer systems and computerized information.

2. SCOPE

This policy covers all unclassified computer systems, including (1) personal computers and word processing systems, (2) computer systems used for scientific and engineering computations, information processing, and experimental control, (3) new, experimental computing systems, and (4) the central computing systems operated by the Computing and Telecommunications Division.

3. POLICY

It is Laboratory policy to protect its computers, the information stored in them, and the sensitive applications running on them. They are to be protected, as far as is reasonably possible, from unauthorized access to applications and computing resources, and unauthorized (or accidental) modification (or destruction) of information. Adequate protection will be based on an evaluation of risks, a cost/benefit analysis of protection measures, and the sensitivity and value of the assets to be protected.

It is Laboratory policy that the primary responsibility for protection of Laboratory computers, programs, and data lie directly with the users, operators, and managers of those Laboratory assets.

It is Laboratory policy that all users, operators, and managers of computing resources be trained in their computer protection responsibilities.

It is Laboratory policy that Laboratory-owned computers be used only for Laboratory-approved work.

4. GOALS

- To protect sensitive computer applications (e.g., accounts payable, personnel, and sensitive DOE energy programs) from unauthorized alteration or disclosure.
- To protect computer systems from deliberate or accidental physical damage.
- To protect computer data and applications from deliberate or accidental modification or destruction.
- To provide adequate and realistic backup procedures and contingency plans that will protect the Laboratory from the consequences of any serious computer failures, and to provide for continuity of operations for computer applications supporting DOE mission-essential functions.

- To prevent the use of Laboratory computers for unauthorized purposes.
- To follow DOE requirements for reporting computer security incidents.

5. RESPONSIBILITIES

The Computing Policy Committee:

- Advises the Laboratory Chief Operations Officer on the suitability of proposed Computer Protection Policies.
- Approves plans for implementing proposed policies.

The Director of Computing and Telecommunications:

- Appoints the ANL Computer Protection Program Manager.

The Site Manager of Argonne West:

- Appoints the Associate Computer Protection Program Manager for Argonne West, ANL Division Directors, Program Managers, and Department Heads;
- Appoints a Divisional, Program, or Departmental Computer Protection Program Representative for each organization.
- Appoints an Assistant Computer Protection Program Manager for each sensitive computer in the organization (one person may be responsible for more than one system). This person is usually (but need not be) the system manager for the computer.
- Ensures that computer security awareness and education training is provided for each organization.

The Computer Protection Program Manager:

- Formulates ANL computer protection policies.
- Prepares the Laboratory's Computer Protection Plan.
- Manages a program to identify sensitive computer applications.
- Manages a program to review, test, and approve protection plans for sensitive applications and computer systems.
- Reviews and approves the computer protection aspects of audit inspections.
- Conducts appraisals of adherence to the Laboratory's Computer Protection Plan.
- Manages a computer security education and awareness program.
- Manages a program to train divisional Computer Protection Program Representatives and Assistant Computer Protection Program Managers.
- Manages the Laboratory's computer-incident reporting system.
- Maintains the Laboratory's computer protection files.

- Coordinates requirements for the unclassified computer protection program with Laboratory personnel having responsibilities for telecommunications security and classified computer security.

- Serves as a Laboratory focal point to coordinate with DOE on matters involving unclassified computer security.

The Associate Computer Protection Program Manager for Argonne West:

- Coordinates computer protection activities at Argonne West to comply with the ANL Computer Protection Program.

- Formulates computer protection policies for Argonne West (in cooperation with the Computer Protection Program Manager).

- Reviews and approves the computer protection aspects of audit inspections at Argonne West.

- Reviews protection plans and conducts appraisals of adherence to the Laboratory's Computer Protection Plan at Argonne West.

- Coordinates the computer security education and awareness training at Argonne West.

- Coordinates Argonne West's computer-incident reporting and subsequent investigations for incidents at Argonne West.

The Computer Protection Program Representatives:

- Charge the manager of each new or significantly changed application to determine the sensitivity of the application and forward that information to the Computer Protection Program Manager.

- Review, approve, and have available upon request risk assessments and protection plans for sensitive applications and computer systems in their organizations.

- Ensure compliance with generic Laboratory risk assessments and protection plans (or write an individual risk assessment and protection plan) for non-sensitive computer applications and systems in their organizations.

- Conduct security-design reviews and tests, and certify and re-certify protection measures for sensitive computers and applications in their organizations.

- Ensure that personnel in their organizations receive computer security education and awareness training.

- Report and document computer security incidents in their organizations in compliance with the ANL Computer Incident Reporting Procedures.

- Review the contents of unclassified divisional computer systems at unannounced intervals with the knowledge and cooperation of division management by random sampling. Document the results, and forward any findings to the Computer Protection Program Manager.

  This review must occur at least annually, but may not cover every computer. The resources used should be commensurate with the loss expectancy.

The Director of Management Information Systems:

- Appoints a Computer Protection Program Representative for systems maintained by Management Information Systems.

- Reviews risk assessments and protection plans for all Laboratory-wide sensitive information-system applications.

The Computer Protection Program Representative for Management Information Systems:

- Charges the manager of each new or significantly changed application managed by Management Information Systems to determine the sensitivity of the application and forwards that information to the Computer Protection Program Manager.

- Reviews, approves, and has available upon request risk assessments and protection plans for sensitive applications maintained by Management Information Systems.

- Insures compliance with generic Laboratory risk assessments and protection plans, (or writes individual risk assessments and protection plans) for non-sensitive computer applications and systems maintained by Management Information Systems.

- Conducts security-design reviews and tests, certifies, and re-certifies security specifications for sensitive applications .

- Insures that personnel in Management Information Systems receive computer security and awareness training commensurate with their responsibilities.

- Manages the documentation and reporting of computer security incidents involving applications maintained by Management Information Systems.

- Reviews and approves the computer protection aspects of audit inspections made on systems maintained by Management Information Systems.

The Assistant Computer Protection Program Managers:

- Prepare and have available on request risk assessments and computer protection plans for each of the sensitive computers for which they are responsible.

  This task can be delegated to the system manager for the computer system and then approved by the assistant, where the two are not the same person.

- Submit the protection checklist for their computer(s) to the Computer Protection Program Manager.

The Managers of computer applications:

- Complete a "Computer Application Sensitivity Questionnaire" for each new or significantly changed application and verify the information as requested by the Computer Protection Program Manager.

- Ensure that adequate back-up protection exists for the application data.

- Comply with protection measures documented in the protection plan.

The Managers of sensitive computer applications:

- Prepare risk assessments and protection plans (and, where appropriate, contingency plans) for each sensitive computer application.
- Insure that the protection of any computer system on which the application runs is adequate for the protection needs of the application.

The System managers of non-sensitive computer systems:

- Insure that the computer system complies with Laboratory policy and procedures for the protection of computing resources.

The Requisitioners of sensitive computer applications or significant computer systems:

- Include appropriate protection requirements in the Procurement specifications.
- Provide completed sensitive computer system or application check lists.

The Procurement Department:

- Ensures that procurement requests for sensitive computer systems and computer applications are in compliance with ANL procurement procedures.

The Human Resources Department:

- Performs normal pre-employment screening checks on prospective employees.

The Internal Audit Department:

- Reviews the contents of the ANL mainframe computer systems at unannounced intervals by random sampling at the request of the Computer Protection Program Manager, and subject to effort constraints.

The Computer Users:

- Provide adequate protection, including proper password selection and protection and data backup, for the applications, data, and computers they use.
- Report computer-security incidents and other suspicious happenings or activities to the proper authority.
- Understand and comply with the ANL Computer Protection Policy and computer protection plans for the applications and computer systems they use.

6. DEFINITIONS:

   a. An application is a set of all computer programs and related data used in an activity or project or closely related set of activities or projects. Examples of individual applications are the Laboratory's Integrated Financial System, the codes used to calculate the energetics and dynamics of molecular systems, and the codes used to determine core neutronics.

   b. A sensitive computer application is an application that requires protection because it contains data that must legally be protected (e.g., Privacy Act Information, Unclassified, Controlled Nuclear

Information, Official Use Only Information) or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application (e.g., payroll, personnel, proprietary code, DOE energy code, reactor control code, substantial financial loss).

c. A sensitive computer system is a computer system that processes sensitive applications or one that qualifies as sensitive because it is significant (see below).

d. A significant computer system is a computer system that consists of a stand-alone computer with peripheral equipment or a network of computer systems. The capacity of the system or network is such that its computing capacity currently requires it to be reported in the annual DOE Information Technology Resources long range planning process.

e. A protection checklist is either of two specific forms. The "Sensitive Application Check List" describes the information needed to complete a protection plan for a sensitive application. The "Sensitive Computer System Check List" describes the information needed to complete a protection plan for a sensitive computer system.

APPENDIX E

ANL PROCEDURE FOR REPORTING COMPUTER SECURITY INCIDENTS

1. REQUIREMENTS

DOE Order 1360.2A describes significant computer security incidents and requires that they be documented and reported to DOE. This document defines the ANL procedures to be followed in reporting all unclassified computer security incidents. Table 1 classifies security incidents according to their severity, using the description of significant from DOE Order 1360.2A, and defines the final reporting authority for each classification of incident.

2. RESPONSIBILITY FOR ADMINISTERING THE ANL COMPUTER PROTECTION POLICY

The primary responsibility for protecting Laboratory sensitive applications and the computers on which they run rests with those persons who operate the computers and those who design, maintain, and use the applications. The Argonne Computer Protection Program Manager is responsible for administering a program to assure the adequacy of and compliance with standards for the protection of unclassified computer systems and applications at Argonne National Laboratory. The Director or Manager of every division, department, or program within ANL appoints a Computer Protection Program Representative who is responsible for ensuring protection policy compliance for the sensitive and critical applications and computers belonging to that division, department, or program. Assistant Computer Protection Program Managers are appointed by division directors and program or department managers for every computer system whose capacity and value require it to be reported in the ANL *Information Technology Resources Long Range Plan.* These Assistants are responsible for the security of those computers and the data and applications residing on them.

3. INITIAL REPORTING OF INCIDENTS

A person who believes a computer security incident has occurred on one of the Laboratory's central computers operated by the Computing and Telecommunications Division should report the incident directly to the Laboratory's Computer Protection Program Manager, who will verify and determine the severity of the incident and will follow these documentation, investigation, and reporting procedures. The Computer Protection Program Manager must report all security incidents involving an ANL employee to the director or manager of the ANL program, department, or division for whom the employee works.

A person who believes a computer security incident involving a distributed divisional computer or workstation has occurred should immediately report the incident to the Assistant Computer Protection Program Manager responsible for the computer on which the incident occurred, or to the Computer Protection Program Representative for the ANL organization involved. The Assistant or the Representative will report all incidents to the responsible line manager. The Assistant or the Representative shall make a preliminary determination of the severity of the incident and shall immediately report incidents of severity level 2 or higher to the Computer Protection Program Manager. The Computer Protection Program Manager will make the final determination of the sensitivity of incidents of severity level 2 or higher and will follow these documentation, investigation, and reporting procedures.

4. SUBSEQUENT REPORTING

The ANL Computer Protection Program Manager will promptly report incidents of level 2 and higher to the Chief Operations Officer, and they, together with the Manager of the ANL Security Department will make the final determination of the severity of those incidents and determine what type of future action (e.g., legal counsel, law enforcement) is required. Severity level 3 incidents are significant, as described in DOE Order 1360.2A, and will be reported by the Computer Protection Program Manager to the DOE using the reporting procedures outlined in the DOE "Computer Security Incident Reporting Procedures."

5. INVESTIGATION AND DOCUMENTATION OF INCIDENTS

The responsible Assistant Computer Protection Program Manager or the Computer Protection Program Representative will investigate level 2 or 3 incidents occurring in the Assistant's or Representative's jurisdiction under the direction of the Computer Protection Program Manager. The Assistant or Representative will prepare a preliminary report to be delivered to the ANL Computer Protection Program Manager within two working days of the incident. When the investigation is complete, the Assistant or Representative will send a final report to the ANL Computer Protection Program Manager to keep as a part of the Laboratory computer protection records.

The ANL Computer Protection Program Manager will investigate incidents occurring on the central computers or applications that are processed on the central computers and will keep on file the final reports of all computer security incidents of severity level 2 and higher for a period of at least three years.

6. ALTERNATE REPORTING POINTS

In cases where the Assistant Computer Protection Program Manager or the Computer Protection Program Representative cannot be located, the person reporting the incident will contact the ANL Computer Protection Program Manager directly.

In cases where the ANL Computer Protection Program Manager cannot be located, the Associate Director for Operations in the Computing and Telecommunications Division shall be notified.

In cases where neither the ANL Computer Protection Program Manager nor the Associate Director for Operations in the Computing and Telecommunications Division can be located, the Director of the Computing and Telecommunications Division shall be notified.

Appropriate personnel and their ANL telephone numbers are:

ANL Computer Protection Program Manager
(L. Jean Troyer) 2-7440

CTD Associate Director for Operations
(L. Michael Boxberger) 2-5638

Director of Computing and Telecommunications
(David P. Weber) 2-7155

ANL Chief Operations Officer
(Ronald J. Teunis) 2-5569

Table 1

Security Incidents and Reporting Authority

	LEVEL	TYPE OF INCIDENT AND REPORTING AUTHORITY
1.	Minor	Unauthorized sharing of user verification passwords; attempts to access a system with little chance of success; inadvertent access to sensitive information; minor abuse of a system by authorized users (e.g., games and recreation). Must be reported to the Assistant Computer Protection Program Manager for the system and to the Director or Manager of the ANL program, department, or division. Incidents on the Laboratory's central computers must be reported to the Computer Protection Program Manager.
2.	Important	Major misuse or abuse of a system by an authorized user (e.g., using the system to support a personal business); penetration of a system by unauthorized, non-ANL persons; deliberate access to or distribution of sensitive information; concentrated attempts to gain access to an ANL computer system. Must be reported to Computer Protection Program Manager, and to ANL Chief Operations Officer.
3.	Significant	Deliberate destruction or unauthorized modification of sensitive or mission-critical data, or any incident that may result in loss, harm, or embarrassment to the DOE; criminal actions which may be prosecuted in the courts; incidents whose reporting could benefit other DOE installations susceptible to the same threats (e.g., security holes in major operating systems). Must be reported to DOE according to DOE-CH requirements.

APPENDIX F

COMPUTING WORKSTATION ACQUISITION JUSTIFICATION

The following ANL-489 form is to be completed for acquisitions costing at least $1,000 but not more than $25,000 for any single computing workstation component:

Argonne National Laboratory

Date:_____

Computing Workstation Equipment, Software, and Peripherals Acquisition Justification

Division or Department_____

Requester_____

Location_____ Phone_____

Requisition Number_____

Estimated Total Cost_____

Procurement Type:

- ☐ ANL Inventory (stock item)
- ☐ Competitive
- ☐ Sole Source (attach ANL-410)
- ☐ Purchase
- ☐ Lease (attach lease/purchase analysis)

(See Reverse Side for Instructions)

I. Description of Need:

II. Functional Requirements and Basis for Selection:

III. Benefits to be Achieved:

IV. Compliance with ANL Computer Protection Policy

A. Will the use of this procurement be in compliance with ANL computer protection policy copyright laws, and protection of the proprietary interests of applicable software vendors? ☐ yes ☐ no

B. Is this aqusition for a sensitive computer workstation or application? (See instructions on reverse.) ☐ yes ☐ no

If yes, you must submit a letter of approval from the ANL Computer Protection Program Manager with this form.

C. Will this equipment or software be used to process classified data? ☐ yes ☐ no

If yes, you must submit a letter of approval from the ANL Computer Site Security Manager with this form?

_____
Requester Signature

Approved_____
Division Director or Department Head

ANL-489 (8-91)

Definition of Terms for Acquisition Justification of ANL Computing Workstation Equipment, Software, and Peripherals

Computing workstation components are personal desktop computers, computer terminals, micro computers, combined voice/data terminals, word processor and office automation electronic workstations, all peripherals such as printers, plotters, and associated software costing less than $25,000. Items valued at or less than $1,000 do not require submission of this ANL-489 form.

I. Description of Need:

Provide a concise statement of what need this procurement is to meet and how this equipment or software will be used.

II. Functional Requirements and Basis for Selection:

State concisely the basis upon which the items proposed for acquisition have been selected. This rationale should include, where possible, the specifications to be met, the compliance with the computer resource strategy of the organization, the compatibility with other equipment, a review of hardware and software available, and the unavailability of equipment in the organization. Specifically address requirements for communication to other computer systems through local area networks, modems, leased lines, etc.

III. Benefits to be Achieved:

State briefly the benefits achieved through this procurement (e.g., provision of new capabilities, reduced operating costs, cost avoidance). Be as specific as possible; where possible, estimate savings in terms of person-months of effort or dollars per year.

IV. Compliance with ANL Computer Protection Policy:

It is Laboratory policy to protect its computers, databases, and the sensitive applications running on them, as well as to insure that Laboratory-owned computers will be used only for Laboratory work (see August 1989, Computer Protection Policy statement as well as *Guide to Computer Protection at ANL*, ANL/TM 413). Furthermore, the Laboratory must protect the proprietary nature of computer software licensing agrements (see R. L. Teunis's memo to all employees, August 20, 1991).

Owners of computer applications and workstations must complete a "Computer Application Sensitivity Questionnaire" to determine whether the application or workstation is sensitive. This form can be obtained from your division Computer Protection Program Representative, must be completed, and must be sent to the ANL Computer Protection Program Manager.

Those purchasing sensitive computers and compter applications must complete a risk assessment and protection plan and have it approved by the division Computer Protection Program Representative. Purchasers of sensitive computers and computer applications must then complete the "Sensitive Computer System or Application Check List," as appropiate, and send it to the ANL Computer Protection Program Manager (CPPM). The CPPM will then send a letter of approval to Procurement with a copy to the requisitioner.

APPENDIX G

PROPRIETARY COMPUTER PROGRAM LICENSES

The following intra-Laboratory memorandum from Ronald J. Teunis, ANL Chief Operations Officer, defines employee responsibilities for complying with computing software licenses:

Argonne
National
Laboratory

Intra-Laboratory Memo

October 3, 1991

TO: All Employees

FROM: R. J. Teunis, Chief Operations Officer

SUBJECT: Employee Responsibilities for Complying with Software Licenses

As you are aware, the unauthorized duplication and use of computer software is contrary to Laboratory and DOE policy and violates the U. S. Copyright Law. Unless otherwise specified in a license agreement, the funds used to purchase a software product represent a license fee for the use of one copy of the software product. Where software is used on a local area network server, all those who have concurrent access to that software on the server must be licensed to use that software. Unless the license is specifically written to include network use, this means that individual licenses must be purchased for every person who concurrently access the software on the server.

Should any software be reproduced, duplicated, or accessed without authorization, then the U. S. Copyright Law has been violated, making the infringement a Federal offense. Civil damages for unauthorized software copying can be as much as $50,000, and additional criminal penalties such as fines and imprisonment can be imposed.

One issue that has been raised within the Laboratory concerns the disposition of obsolete shrink-wrapped software (software bought without a specific applicable license) for personal computers and work stations. The Laboratory now recommends that users can: 1) keep such software on file within the organization; 2) reformat the floppy disks and reuse them, or 3) reformat and discard the floppy disks. When you discard or reuse such software, your division should keep a record on file noting the date and method of disposition. This record should be attached to or (in the case of electronic record keeping) associated with the purchase order.

RJT:bc

APPENDIX H

USE OF COMPUTERS AT ANL

A copy of a document all new ANL employees must sign appears on the following page. When signed, this document affirms computer user understanding and responsibility for protecting copyrighted or patented materials from misuse. It also affirms the user's understanding of security responsibilities.

NAME:_____ BADGE:_____

Use of Computers at
Argonne National Laboratory

It is Laboratory Policy:

1. To protect sensitive computer applications (such as accounts payable, payroll, personnel, and sensitive DOE energy programs) from unauthorized alteration or disclosure.

2. To protect computer systems from deliberate or accidental physical damage.

3. To protect the Laboratory from the consequences of serious computer failures or destruction, through adequate and realistic backup procedures and contingency plans.

4. To prevent the use of Laboratory computers for unauthorized purposes.

Computers and computer systems include word processors, workstations, terminals, and personal computers as well as divisional and Laboratory mainframe computers.

Argonne's computers are provided solely for the purpose of carrying out Laboratory work (including authorized work of other agencies). Laboratory work consists primarily of assigned technical and management activities, but it also includes professional development, training, and other Laboratory approved activities undertaken with the knowledge and approval of your supervisor. Laboratory computers may not be used for purposes that are of a personal nature, such as for a private business.

Certain sensitive data are stored on some computers. No one may access or attempt to gain access to such data unless specifically authorized to do so. However, if you inadvertently gain access to sensitive information, you must inform your supervisor and the Computer Protection Program Manager in the Computing and Telecommunications Division. Similarly, should you receive misdirected output that is not sensitive, simply return it to the place where you obtained it. However, when you believe that misdirected output contains sensitive information, please notify your supervisor and forward the output to the Computer Protection Program Manager.

If you yourself use a computer system that processes sensitive data, you must protect that data, both inside the computer and when it has been printed. If you develop a computer system that processes sensitive data, you must follow the prescribed procedures described in ANL/TM 413, Guide to Computer Protection at ANL, obtainable from the Computing and Telecommunications Division.

To assure that users of computers are who they claim to be, the Laboratory has implemented validation methods that require passwords to use computers shared by many users. You should not share or divulge your password. You should change your password regularly -- at least every six months. If your work involves sensitive data you may need to change your password more frequently. You are responsible for the integrity of your password. Choose one which is not easily guessed by others. Memorize your password so you will not need to write it down where others might find it. If you believe your password has been compromised, you should change it immediately.

You should inform the Computer Protection Program Manager when (a) you believe the security mechanisms are not working properly, or (b) you suspect that someone is deliberately trying to break into the system, or (c) you have inadvertent access to sensitive information.

I have read and understood the foregoing policy. I further understand that disciplinary action, up to and including discharge, can result from failure to comply with the provisions of this policy.

signed_____ date_____

LJT:lem 09/20/88

REFERENCES

1. ANL Support Services Division. *Procurement Procedure No. 44. Computing Workstation Components*, Argonne: Support Services Division, October 1988.

2. Boxberger, L. Michael. *ANL Site Response for the DOE FY1993 Information Technology Resources Long-Range Plan* (ANL/TM 485). Argonne: Computing and Telecommunications Division, February, 1991.

3. Boxberger, L. Michael. *ANL Statement of Site Strategy: for Computing Workstations* (ANL/TM 458, Revision 2) Argonne: Computing and Telecommunications Division, Revised September, 1989.

4. Kolsto, Elliot L. and Richard J. Royston. *Guide to Computer Protection at ANL* (ANL/TM 413). Argonne: Computing Services, February, 1984.

5. O'Brien, Diane E. *et al. A Plan for Administrative Computing at ANL:FY1992 through FY1994* (ANL/TM 489). Argonne: Computing and Telecommunications Division, October 1991.

6. U. S. Department of Energy. *DOE Order 1360.1A: Acquisition and Management of Computing Resources.* Washington, D. C.: U.S. Department of Energy, May 30, 1986.

7. Winkler, Linda. *Guide to Sharing Personal Computer Resources via Local Area Networks* (ANL/TM 438). Argonne: Computing Services, Revised August 1986.

END

DATE
FILMED
01/16/92