

Department of the Interior Departmental Manual

Effective Date: 7/6/93

Series: Information Resources Management

Part 376: Automated Data Processing

Chapter 12: Workstations, Microcomputers, and Computer Networks

Originating Office: Office of Information Resources Management

376 DM 12

12.1 Purpose. This directive establishes policy and defines necessary management controls and guidelines for the acquisition, management, operations, and support of workstations (Class I and Class III systems), microcomputers (Class II systems), and computer networks. It includes responsibility for the development of open systems environments (OSE) and architectures with systems components which adhere to the Government open systems interconnection profile (GOSIP) and portable operating systems interface for computer environment (POSIX) standards.

12.2 Objectives. The objectives of this directive are to:

A. Establish an effective management and support framework which will accommodate flexible acquisition and innovative application of appropriate Class I, II and III systems and computer network technology, while maintaining necessary management controls.

B. Achieve and maintain optimum levels of compatibility, portability, interoperability, and scalability through open systems architecture which is GOSIP and POSIX-compliant to encourage sharing of technology, applications, software, and data resources throughout the Department of the Interior.

12.3 Definitions.

A. Class I System: Intelligent Workstation (Greater Than 16 Bit). A Powerful, specialized workstation with integral capabilities such as graphics, communications (with or without voice), large memory, and local file storage capabilities. These devices are often used for scientific, engineering, or artificial intelligence applications.

B. Class II System: Microcomputer (16 bit or Lower). A general purpose computer consisting of one or more microprocessors assembled in a unit of desk top or smaller size, capable of supporting a number of peripheral devices. The unit typically has a keyboard, video screen, and at least one disk drive.

C. Class III System: Non-Intelligent Workstation. A fixed-function device having no programmability or communications capability except possibly to a controller to which it is attached.

D. Computer Network. A grouping of Class I, II, and III systems and shared peripheral devices connected via direct wiring or a local area network. (Note: A computer network includes all information technology devices, telecommunications facilities connecting these devices, and all network control and application software.)

E. FIPS Programming Languages. Federal Information Processing Standard (FIPS) programming languages which are approved for Governmentwide use. These languages are designed to facilitate application portability and maintainability irrespective of the technology environment in which the applications are to operate.

F. GOSIP, Version 2. Reference FIPS 146-1. A common set of data communication protocols which enable systems developed by different vendors to interoperate and enable users of different applications on these systems to exchange information. It allows users the ability to incorporate communications facilities in such a way as to promote interoperability and connectivity.

G. Instrumentation Systems. Those that are used in conjunction with or used to control laboratory instruments or equipment or to provide specialized data collection or manipulation, as in navigational and surveillance equipment. These systems often have embedded Class I, II or III systems or attach directly to general purpose information technology. (Note: Instrumentation systems are subject to the same regulations as information technology *only* in the computer portion is separable from the instrumentation system.)

H. Licensing Agreement. The contractual terms and conditions by which a buyer or user of proprietary software or data agrees to abide for the privilege of using the software or data. License agreements are normally explicitly stated within the documentation accompanying the proprietary software or data, but when large quantities are involved, different terms and conditions may be separately negotiated as a part of the acquisition process.

I. Microprocessor. The portion of the Class I and II system which provides the control, logic, and arithmetic capability. It is usually manufactured in a single large-scale integrated circuit chip or 8, 16, 24, 32-bit, or higher architecture.

J. OSE. A conceptual framework for developing an open systems architecture with (1) portability (the ability to use applications software and data on heterogeneous hardware/software platforms.), (2) interoperability (the ability to have applications software operating on heterogeneous hardware/software platforms cooperate in performing functions), and (3) scalability (the ability to use the same application software on many different classes of hardware/software platforms, from personal computers to super computers).

K. POSIX. Reference FIPS 151-1. Standard interfaces to an operating systems which allows applications to be ported among heterogeneous POSIX operating systems. POSIX is an attempt to specify a standard set of program calls and command line interfaces for an operating system.

L. Process Control Systems. Those systems that are used for real-time regulation of physical or chemical processes in production situations. Many such devices have embedded Class I, II, or III systems which function much like general purpose microcomputers and thus are subjected to policies defined in this DM chapter. (Note: Process control systems are subject to the same regulations as information technology *only* if the computer portion is separable from the process control system.)

M. Proprietary Software and Data. Commercially available proprietary software and proprietary commercial data bases are usually copyrighted, and all rights are reserved to the copyright owner. Unless otherwise authorized, and copying, duplicating, selling, or other unauthorized distribution of the software or data may be unlawful. Willful violations of the Copyright Law of the United States can result in civil damages of up to \$50,000 in addition to actual damages (17 USC 504 (c)(2)), plus criminal penalties or up to 1 year imprisonment and/or a \$25,000 fine (18 USC 2319 (b) (3)). These same restrictions may pertain to software or data which is neither owned by the Federal Government nor available in the public domain.

N. Sensitive Application. An application of information technology that requires protection because it processes sensitive data or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation. (Ref. FIRMR 201-4)

O. Sensitive Data. Data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act (OMB Circular A-130). This definition also includes confidential information which the Department or bureaus collect from the private sector or public, with the implied understanding that this information will be used only for limited purposes such as statistical analysis, and will not be generally released.

P. Technology Life Cycle. The time period beginning with formal articulation of a requirement for a general or specific type of technology to meet a mission requirement and ending with the final disposition of the technology item(s) acquired to support the requirement.

12.4 Applicability. The policies and responsibilities defined within this directive apply to the acquisition, management, operation, and support of all Class I, II, and III systems and computer networks, unless otherwise noted, within the Department of the Interior. This directive also applies to authorized agents, including commercial contractors and universities, performing mission or administrative functions on behalf of the Department.

12.5 General Policies. It is the Department policy to utilize Class I, II, and III systems and computer networks, as appropriate, to cost-effectively support mission and administrative functions, and to improve personnel and organizational productivity. It is also the Department's policy to acquire, implement, control, and support Class I, II, and III systems and computer networks through the execution of well-planned management strategies. These management

strategies include:

- A. An established set of management responsibilities and accountabilities;
- B. A defined methodology for planning and requirements analysis;
- C. An Information Resources Management (IRM) Strategic Plan (reference 375 DM 4);
- D. Use of FIPS (including GOSIP and POSIX) where applicable;
- E. An application and configuration management process;
- F. An acquisition plan;
- G. An installation/training plan;
- H. Operational controls including security controls; and,
- I. User support and hardware maintenance strategies.

12.6 Responsibilities.

A. Office of Information Resource Management (PIR). The Director, PIR, will exercise Departmental oversight over Class I, II, and III systems and computer network management; formulate policies, guidelines, and standards for all system classes and computer networks; issue reports as required; and conduct acquisition reviews, approvals, and assessments of all system classes and computer network management and use. The Director also will coordinate Departmentwide Class I, II, and III systems and computer network requirements and applications, as needed, and carry out the specific IRM responsibilities stated in 12.6 B (below) for the Office of the Secretary and other Departmental offices.

B. Heads of Bureaus. Heads of Bureaus are responsible for:

- (1) Implementation of Departmental Class I, II, and III systems and computer network policies within their respective bureaus;
- (2) Accomplishment of adequate planning and requirements analysis prior to selection and acquisition of Class I, II, and III systems and computer networks;
- (3) Integration of requirements and consolidation of acquisitions to the maximum practical extent. At a minimum, integration of requirements should occur within specific program areas or administrative areas (e.g., finance) within each bureau;
- (4) Establishment of operational, security, and accountability controls for Class I, II, and III systems and computer networks;
- (5) Maintenance of bureau inventories of Class I, II, and III systems, computer

networks and associated peripherals, and submission of inventory data and reports to PIR, as required, to support Departmental management and reporting requirements;

(6) Provision of adequate network planning support and assistance in the acquisition of telecommunications equipment and services, including development of plans to integrate current and planned installations of Class I, II, and III systems;

(7) Adherence to FIPS for the acquisition of product components which meet GOSIP and POSIX-compliant standards;

(8) Adherence to Departmental and bureau IRM standards; and

(9) Adherence to Federal, DOI, and bureau records management requirements.

C. Program Managers and Administrators. Program managers and administrators are primarily responsible for the overall application and management of Class I, II, and III systems and computer networks used in support of their assigned mission/administrative responsibilities. Program managers and administrators will:

(1) Ensure that the Departmental and bureau Class I, II, and III systems and computer network policies are adhered to;

(2) Identify application, systems performance, communications, and security requirements for Class I, II, and III systems and computer networks;

(3) Implement management controls and accountability for Class I, II, and III systems and computer networks, including controlling interfacing between system classes and computer networks and minicomputers or mainframes;

(4) Maintain compatibility of Class I, II, and III systems, computer networks, applications, and data through implementation of OSE concepts and adherence to GOSIP and POSIX standards where applicable, including maintenance of technological and application compatibility with all mainframes or minicomputers that are accessed by Class I, II, and III systems and computer networks;

(5) Ensure that Class I, II, and III systems and computer network users performing program/administrative functions are adequately trained; and

(6) Ensure adequate planning is accomplished in the creation, handling, and disposition of automated records to meet records life cycle management requirements.

D. Users. Users are responsible for the operational control, security, and proper utilization of the systems and computer networks, which they use exclusively or share with other users. Users will:

(1) Maintain individual hardware and software (when the cost exceeds \$300)

inventories, report to your local Property Management unit any changes that occur in your inventory due to transfers to other employees, or replacement of equipment through maintenance contracts, account for costs and assess utilization of the systems and computer networks, in accordance with bureau policies. (Reference 12.10A(2), (3), and (6));

(2) Protect Class I, II, and III systems, computer networks and associated peripherals, software, and storage media against damage or loss and unauthorized use;

(3) Properly operate and utilize Class I, II, and III systems and computer networks in accordance with Departmental and bureau procedures, including following established procedures for records management;

(4) Secure and protect sensitive and Privacy Act data stored or processed within Class I, II, and III systems and computer networks;

(5) Protect from disclosure data such as telephone numbers and passwords which provide Class I, II and III systems and computer networks access to minicomputers, mainframes, or other telecommunications networks;

(6) Strictly observe all license agreements for proprietary software or data.
(Reference 12.10A(1))

12.7 Planning and Requirements Analysis.

A. Planning. Planning for the acquisition and application of Class I, II, and III systems and computer of Class I, II, and III systems and computer networks must be accomplished in accordance with approved Departmental and bureau strategic plans. Major procurement actions must be identified in the bureau's IRM Strategic Plan (reference 375 DM 4 for strategic planning requirements). In addition, budget requirements must be included pursuant to Office of Management and Budget Circular A-11, Exhibits 43A and 43B.

B. Requirements Analysis. Bureaus will conduct requirements analyses, feasibility studies, and benefit/cost analysis *commensurate with the size and complexity of each planned Class I, II, or III system or computer network acquisition*.

C. Integration of Requirements. The scope of planning and requirements analysis should cover the broadest possible organizational unit, program or mission area, administrative, or other functional activity to ensure achievement of compatibility through the use of GOSIP and POSIX, where applicable. Acquisitions that satisfy short-term or immediate requirements within a specific program area should not override meeting longer term needs of the entire program or organization without clear justification to do so.

12.8 Application and Configuration of Class I, II, and III Systems and Computer Networks.

A. General. Class I, II, and III systems are to be used to improve the productivity of

individuals and/or organizations in the collection, analysis, preparation, processing, and reporting of data including text, numeric or image (graphic/multi-media) data, or combinations thereof. In a network environment they are to be used to share common facilities (e.g. printing or storage) where practical, share or exchange data and applications software (non-proprietary only, unless permitted under license agreement), and facilitate interorganizational communications and common administrative processes.

B. Proper Application of Class I, II, and III Systems and Computer Networks. Class I, II, and III systems and computer networks will be applied to processes which can be cost effectively automated at the individual user level. They may also be incorporated as a part of larger (multi-user) application environments to support functions such as off-line or interactive data entry or data extraction (from a host system), to support the need for distributed data access, and to facilitate data analysis.

C. Configuration of Class I, II, and III Systems. Configuration of Class I, II, and III systems should be based upon consideration of all relevant current and future performance requirements, application needs, and technology changes which are likely to occur during the planned life of the system. Part of the configuration process may be appropriately deferred to the acquisition process, with bids or offers solicited for various configuration options.

D. Application Systems. Application systems will, to the maximum practical extent, consist of commercially available off-the-shelf software which are supported by the original software supplier or authorized vendor representative. Application systems which must be developed should be programmed in one of the preferred FIPS programming languages unless otherwise justified. Bureau IRM managers, in close coordination with program managers and administrators, should exercise strong central control over development and maintenance of multi-user applications to ensure adherence to FIP standards and maintenance of compatibility. Bureaus should also exercise diligence in application systems development to minimize redundancy. Nonproprietary software should be readily exchangeable among bureaus and offices, using electronic transfer where feasible to facilitate this process.

12.9 Acquisition of Class I, II, and III Systems and Computer Networks.

A. General. To assure orderly acquisitions of Class I, II, and III systems and computer networks bureau will:

- (1) Follow established Federal and Department of the Interior procurement policies and procedures including information technology procurement policies provided in 376 DM 4;
- (2) Promote the migration to OSE through procurements which ensure that GOSIP and POSIX requirements are properly integrated and consolidate acquisitions when appropriate;
- (3) Perform requirements analyses, feasibility studies, and benefit/cost analyses commensurate with the size and complexity of the acquisition (as defined in 375 DM 7);
- (4) Correlate bureau acquisition plans with mission plans.

B. Acquisition Strategies. Bureaus will develop long-term strategies for the acquisition of Class I, II, and III systems and computer networks. Acquisition strategies must be periodically reviewed and revised as necessary to reflect changes in technology and the commercial market. Major acquisition plans for Class I, II, and III systems and computer networks must be identified in the bureau's information technology budget and IRM Strategic Plan. Bureaus should strive to consolidate acquisitions of systems and computer networks where feasible and cost effective. Acquisition strategies should be periodically reevaluated to consider changes in technology and the marketplace and should be adjusted as necessary to provide an optimum balance among the considerations of compatibility, portability, interoperability, scalability, economies of scale, flexibility, delivery requirements, performance requirements, and administrative overhead. Bureaus should ensure that GOSIP and POSIX requirements are properly integrated in acquisitions.

C. Acquisition Approval Requirements. The acquisition of Class I, II and III systems, computer networks, and related support services are subject to Federal and Departmental information technology procurement policies and procedures. Departmental information technology procurement policies and approval requirements are specified in 376 DM 4 and 377 DM 1. Bureaus will develop policies and procedures for the acquisition of systems and computer networks which fall below Departmental approval thresholds. Emphasis should be given to simplification of the justification and approvals for Class I, II, and III systems and computer network purchases involving low dollar amounts. Bureau requirements for Class I, II, and III systems and computer networks shall not be split into multiple acquisitions to circumvent Departmental review and approval.

12.10 Operations. Bureau IRM managers, program managers, administrators, systems, and computer network users will ensure that adequate operational controls and guidelines are established and followed. The controls and guidelines established will be in conformance with the following policies.

A. Operational Controls.

(1) Control and Use of Proprietary Software and Data. Bureau will ensure that Class I, II, and III systems and computer network users are aware of the restrictions on use and duplication of proprietary software and data. Also, each user should be required to maintain, as part of the site inventory and operational guidelines, a list of user authorized proprietary software packages (when the cost exceeds \$300) and accessible data bases. Bureaus should ensure that proprietary software or data license agreements requiring written signature confirmation are executed only by authorized bureau officials having delegated authority to sign such agreements.

(2) Inventory/Documentation Requirements. Bureau will ensure that Class I, II, and III systems and computer networks (when the cost exceeds \$300) are accounted for in the bureau's property system.

(3) Utilization and Effectiveness of Class I, II, and III Systems and Computer Networks. Bureaus will periodically assess the utilization and effectiveness of each system and

computer network. Utilization guidelines should be established for each major application type or functional area (e.g., Class I, II, or III systems for financial applications, Class II, or III systems for secretarial word processing.) These guidelines should be used to plan requirements for new systems and computer network acquisitions and to assess utilization levels. The ratios of Class I, II, and III systems to users and other relevant guidelines should be based upon such factors as the volume of work, major application functional area, technology costs, mission criticality, physical accessibility, and security considerations.

(4) Maintenance. Bureau will establish guidelines for end-user to follow in the acquisition and performance of maintenance services. The maintenance guidelines should identify and categorize maintenance related activities and provide end-users with options and criteria to apply in selecting cost effective maintenance support. The guidelines should cover at a minimum:

- (a) End-user diagnostic and maintenance functions;
- (b) Maintenance support through DOI information technology centers; and
- (c) Commercial maintenance services alternatives.

(5) Records Management. Controls for creation, retention and disposition of automated data, software, and related files shall comply with approved records schedules. (Reference specifically 382 DM 11, Managing Records in Electronic Form.)

(6) Cost Accounting. Bureaus shall maintain records, consistent with the size and complexity of the installation, which show the life cycle costs associated with Class I, II, and III systems and computer networks. These records should include the initial acquisition cost of the systems, computer networks, peripherals, software, maintenance and related support facilities, plus the cost of any add-on features or augmentations throughout the life of the system and computer network. Records of both capital investment costs as well as annual support costs (excluding user salary/benefit costs) are to be maintained.

(7) Use of Personal Computers and Use of Government-owned Class I, II, and III Systems at Home. Bureaus may, at their discretion, permit employees to bring their own personal computers to the office or to take Government-owned Class I or II systems home for authorized purposes, provided such authorization is in accordance with 410 DM 114-60.201. If bureaus permit such use, the following minimum controls are necessary:

- (a) The employee should be required to obtain the written permission of the immediate supervisory and the Accountable Officer;
- (b) Security procedures and risk assessments should be *reexamined* to ensure that security controls are not degraded and risks increased. Bureaus should strongly consider *not permitting* access to highly sensitive data via Class I and II systems and computer networks from employees' homes or other uncontrolled physical sites;
- (c) Employees should be advised that the Government is not responsible for

protection of an employee's personally-owned computer unless such liability is specifically defined and assumed in writing by authorized bureau officials (see 410 DM 114-60.201 (d)(3)). However, the employee is responsible for protection of Government-owned equipment when taken off-premises and may be held liable for damage to or loss of this property.

(d) Both user property records and bureau personal property system records should be carefully maintained to identify current locations of all equipment and software. It is the user's responsibility to keep Property Management informed of any changes in equipment, software, or location that occur informally or through maintenance contracts. Employees should be advised that all job-related information developed and maintained on a personally-owned computer is a Government record and will be maintained and disposed of in accordance with bureau and Departmental records management procedures;

(e) Bureaus should ensure that managers maintain proper accountability and performance controls over employees who use Class I or II systems at home to perform official Government work functions. Managers should also ensure that employees' personal computers conform to essential technical and security requirements prior to authorizing their use for official Government functions.

B. Security. The security of Class I, II, and III systems and computer network installations places clear accountabilities and constraints on managers and users. All bureau managers and users must maintain familiarity with Departmental and bureau security policies and guidelines including obtaining proper ADP security clearances, development of continuity of operations plans, and performance of required risk analysis. (Reference 375 DM 19)

12.11 **Training.**

A. Bureau Training Plans. Prior to installing a new Class I, II, or III system or computer network, bureaus will conduct an assessment (1) of the skills that are required to operate the system(s) and (2) the training needs required to bring the skills of the person(s) assigned to use the system(s) to the appropriate level, in order to operate the equipment effectively and efficiently. Bureaus will also develop ongoing training plans to develop and maintain adequate levels of literacy and proficiency in the operation and use of systems and computer networks. As a minimum, the development of training plans should consider:

- (1) Basic computer literacy training for all unskilled or first-time Class I, II, or III system and computer network users;
- (2) Basic training in IRM Security responsibilities;
- (3) Training in data management covering the accessing and sharing of data;
- (4) Basic training in Departmental and bureau information technology management and operational policies, procedures, and guidelines to include training on electronic records, and property management responsibilities;

(5) Training covering specific application and Class I, II, and III system and computer network technology products which will be used in that office; and

(6) Training on applications design, programming, and testing for users who will be developing or customizing applications programs.

B. Sources of Training. Bureaus may utilize a combination of training sources; however, internal sources must be consulted first before commercial sources are sought. Quality of training and special training needs should be considered as well as cost in selecting the appropriate training source. Training should normally be sought in the following order:

(1) Departmental Learning Center, located in Washington, D.C., Main Interior Building, and *established* bureau in-house training facilities.

(2) DOI information technology centers.

(3) Other Government training centers such as GSA or OPM.

(4) Commercial training sources.

12.12 Standards and Guidelines.

A. Minimum Standards. All Class I, II, and III systems and computer networks acquired after the effective date of this DM chapter will conform to Federal and Departmental standards unless a specific waiver is granted by the Secretary or Deputy Secretary and the Secretary of Commerce, if required. Requests for waivers should be submitted to PIR for processing within the Office of the Secretary and coordination with the Department of Commerce (for waivers to Federal standards). Waiver requests should be submitted a minimum of 90 days in advance of a planned acquisition or order placement to preclude possible delays in satisfying mission requirements. Future acquisitions of Class I, II, and III systems and computer networks will conform to new Federal and Departmental standards as they are issued.

B. Guidelines. Bureaus should (1) establish supplemental guidelines where appropriate to ensure effective management controls are in place that advance the OSE goals of compatibility, portability, interoperability, and scalability and (2) optimize cost effective applications and use of Class I, II, and III systems and computer networks.

7/6/93 #2980

Replaces 2/17/88 #2779