

OFFICE of the SECRETARY OF DEFENSE

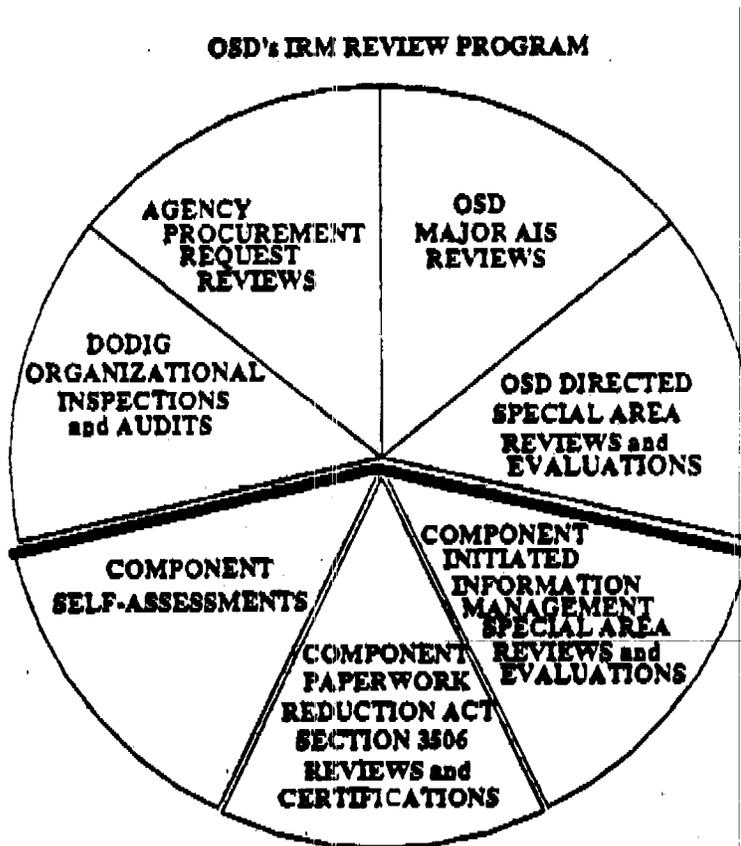
GUIDE for ASSESSING

**COMPONENT INFORMATION MANAGEMENT
ACTIVITIES**

PREFACE

The Paperwork Reduction Act of 1980, as amended, requires Federal agencies to conduct periodic reviews of their information management (IM) activities. The Office of the Secretary of Defensels (OSD) program has been satisfying this requirement by requiring DoD Components to conduct management reviews and evaluations of their IM activities, by conducting OSD management oversight reviews of major automated information system (AIS) programs, and through audits conducted by the DoD Inspector General and Military Department Audit Services. In the future, OSD will also, be asking Components to conduct self assessment IM reviews. OSD will measure its oversight progress in achieving GSA and DoD-priorities and objectives through continuing to require Components to conduct IM reviews in selected areas, conducting major AIS reviews at the OSD level, continuing to require Components to describe and document the results of their own IM reviews, and by instituting this self assessment program. As shown below, the OSD will continue to place major reliance on Component-conducted assessments, reviews and evaluations.

OSD's ERM RENIM PROGRAM



OSD's program for monitoring Component compliance will include DODIG assistance. The major monitoring process will be a Component's certification, based on a self-assessment, with DoDIG random validation. It is intended that each Defense agency will be reviewed and each Military Department's review program will be evaluated once every three years. The initial assessments will be considered the agency's IM compliance baseline. Subsequent assessments will focus on either progress in making identified improvements and/or updating their IM compliance baseline. Assessments are to be documented with each assessed area noting appropriate findings and what improvement opportunities exist. Any IM area not assessed should be identified and explained. Copies of completed certification assessments and validations are to be forwarded to the Program Oversight Office of the Deputy Assistant Secretary of Defense (Information Systems). Also forwarded should be a list of (1) all corrective actions to be taken or (2) improvement opportunities to be pursued and a milestone schedule for accomplishing these activities. In addition, the Component should identify how they are accomplishing the required Section 3506 certification, particularly if the required reviews are being spread over a three-year period. Finally, the Component should include in its reports to Program Oversight a list of the Internal Management Control (IMC) Program reviews completed in the last two years.

The Component's IM programmatic self-assessment reviews should be considered in the execution of their IMC program and DoD's implementation of the Federal Managers' Financial Integrity Act (FMFIA). The IMC Program is implemented through DODD 5010.38, "Internal Management Control Program." These self-assessment reviews, and responses, to review questions, should serve as a major information contribution to the required evaluations of the IMC Program. The questions in this document, in effect, specify numerous internal controls which are applicable to the requirements of the IMC Program. It is noteworthy, to recall that the Deputy Secretary of Defense, in 1991 and again in 1992, specified that the statutory requirements of FMFIA are applicable to all DoD managers.

Information gathered through these self-assessments would usually be an integral part of fulfilling IMC Program requirements. Therefore, the results of this examination can be relied upon when developing Risk Assessment ratings for assessable units and the satisfaction of any subsequent IMC Review requirements, as required by the IMC program. To the extent that these reviews are applicable to a manager's specific IM management responsibilities, the information gathered through these self assessments would serve as an effective data base when drawing IMC Program conclusions. For many IM managers, the foregoing consideration should have a substantial labor-saving impact.

The questions that have been selected for this program reflect consideration of similar programs at the Departments of Army, Energy, Health and Human Services, and Treasury as well as the Agency for International Development and the General Services Administration. Also, assistance has been provided by policy focal points in OASD's P&L, FM&P and C31(CI&SCM) and WHS and DMSSC.

OSD IM SELF ASSESSMENT
BASIC QUESTION AREAS

- A. ORGANIZATION STRU
- B. STRATEGIC IM PLANNING
- C. LIFE-CYCLE MANAGEMENT
- D. HARDWARE AND SOFTWARE MODERNIZATION
- E. TELECOMMUNICATIONS
- F. RECORDS MANAGEMENT
- G. REPORTS MANAGEMENT
- H. FORMS MANAGEMENT
- I. MAIL MANAGEMENT
- J. INFORMATION SYSTEMS SECURITY
- K. ADP/DPA MANAGEMENT
- L. OVERSIGHT/DELEGATION OF AUTHORITY
- M. EFFECTIVE CONTRACT ADMINISTRATION
- N. REVIEW OF SELECTED CONTRACT FILES
- O. COMPONENT IM REVIEW PROGRAM
- P. COMPUTER ACCESS BY USERS WITH DISABILITIES
- Q. CIM POLICY ISSUES

OSD IM ASSESSMENT BASIC QUESTIONS

A. ORGANIZATION STRUCTURE

The Paperwork Reduction Reauthorization Act of 1986 requires agencies to integrate and establish accountability for their information management (IM) activities. DODD 7740.1, "DOD Information Resources Management Program," requires each DOD Component to designate a senior IRM official (or representative) and provides for establishment of coordinated and integrated DOD IM activities.

1. Are all IM functions located in one organization? If not, can the line of accountability and responsibility be traced from senior IM manager to the various IM functional areas?
2. If so, what inspections/reviews have been used by the central IM organization to verify compliance with DOD and Component-wide policies.
3. Does a central IM organization promulgate overall policies and guidance for the management and acquisition of information technology resources on a Component-wide basis? Do these policies amplify the DoD/GSA/OMB directives, instructions, regulations, circulars, etc. on the acquisition and management of information resources?
4. Does a central organization promote Component-wide policies for major IM initiatives such as consolidated contracts, standardization of hardware and software, networks for data sharing, modernization of technology and systems and centralized administrative systems?
5. Do organization charts and mission statements reflect the actual structure and processes?
6. Does the central IM organization have copies of the current version of the Federal Information Resources Management Regulation (FIRMR) and the applicable DOD directives and instructions on IM and life-cycle management? How does the Component ensure that sub-Component users maintain up-to-date copies of these documents?

B. STRATEGIC PLLNNING

Federal agencies are required by the Paperwork Reduction Reauthorization Act of 1986, Office of Management and Budget Circular (OMB) A-130, "Management of Federal Information Resources," and the Federal Information Resources Management Regulation (FIRMR) to develop and revise annually a five-year plan for meeting their information technology needs. DODD 7740.2, "Automated Information System (AIS) Strategic Planning,"

November 1992

requires DoD Components to develop and annually revise an AIS strategic plan. Component performance in strategic planning is a major factor GSA uses when making determinations for granting specific and blanket delegations of procurement authority to agencies.

1. Does the Component have an overall strategic plan for the Component and how is the AIS strategic plan linked to it? Have these plans been updated in the last 12 months? If not, when were they last updated?
2. Are long-range planning submissions developed by functional managers and users? Are they mission-based or related to program goals? Do they include major IM support functions (major information systems, information technology, budget, acquisitions, inventories)?
3. Does the IM organization develop long-term strategies, objectives, assumptions and constraints for sub-Component organizations to use when they develop their strategic plans?
4. How are IM goals and strategies developed and prioritized? How are they then incorporated into a process for managing and monitoring day-to-day IM operations? When new unplanned IM initiatives arise how are they incorporated into existing plans, goals and strategies and accomplished?
5. Are plans reviewed and analyzed by the headquarters IM organization to ensure conformance to DoD and Component policy requirements? Is the strategic planning process top-down with bottom-up input?
6. Are Component-wide functional business and mission plans analyzed and used by the IM organization to develop a Component-wide Strategic AIS Plan?
7. Does Senior IM management approve the Component's Strategic sub-Component AIS plans? How are approved plans then supported by senior management?
8. How is the final plan used to approve major acquisition requests, software development efforts, and other major IM initiatives? How does the headquarters IM organization track progress against the final plan?
9. How are the cost estimates for IM initiatives derived? How does this estimating process relate to the strategic planning and budget formulation process?
10. What is used to monitor progress of a project against milestones? How are past plans and budgets compared to actual performance?

C. LIFE-CYCLE MANAGEMENT

The life-cycle management (LCM) process is for the identification of measurable actions which together will provide for effective, timely, and cost effective design, development, deployment, and use of automated information systems. LCM applies to all development and operational approaches whether they be grand design, incremental or evolutionary in nature.

1. What are the most recent copies of the following documents and related amplifying/implementing Component guidance on hand:
 - a. DODD 7920.1 "Life-Cycle Management of Automated Systems (AISs)"
 - b. DODI 7920.2 "Automated Information System (AIS) Life-Cycle Management Review and Milestone Approval Procedures it
 - c. DoD Manual 7920.2-M "Automated Information System Life-Cycle Management Manual"
 - d. DODD 7740.1 "DoD Information Resources Management Program"
2. What is the Component-wide policy for establishing Component oversight of AISs? Are formal reviews conducted and what are the thresholds/conditions that cause the reviews to occur?
3. Is a single organization responsible for AIS oversight and reviews? If not, what are the responsibilities for oversight and to whom are review results reported?
4. What documents are available to demonstrate the results of Component and OSD-level AIS LCM reviews?
5. Does the Component have a current copy of the Office of the Assistant Secretary of Defense (C3I) designation of major AIS, as defined in DODD 7920.1, memorandum available?
6. Are copies of the Component's major AIS, as defined in DODD 7920.1, quarterly reports (RCS 'L799) on-hand and how are they used?
7. How are AIS programs and federal information processing resource acquisitions evaluated for consistency with CIM plans, CIM technical reference and other standards?
8. How does the agency conduct periodic reviews of operational systems to assure that they are still needed and are still satisfying user needs? How are these reviews documented?

D. AND SOFTWARE MODERNIZATION

Components should continually evaluate their existing outdated federal information processing (FIP) resources to determine whether the cost of operating them is greater than the cost of

November 1992

acquiring and operating technologically newer resources. When the costs of operating existing outdated resources is greater, agencies are required to replace the existing outdated resources. (See FIRMR 201-22.303(b).)

1. Does the Component have any policies and procedures pertaining to the evaluation and management of obsolete FIP resources? How are they related to strategic planning?
2. Does the Component consider the cost of maintaining outdated FIP equipment in the analysis of alternatives for a proposed new acquisition? Are decisions supported by economic analyses?
3. How does the Component conduct obsolescence reviews?
4. Does the Component have any modernization initiatives? Modernization, is any change or modification to an existing AIS or IM resource that results in improved capability or performance.
5. How does the Component maintain an accurate inventory?

E. TELECOMMUNICATIONS

Components are required by DODD 4640.13, "Management of Base and Long-Haul Telecommunications Equipment and Services," and IDODI 4640.14, "Base and Long-Haul Telecommunications Equipment and Services," to ensure effective, efficient, and economical use of base and long-haul telecommunications equipment and services.

1. What processes does the Component use for the identification of new telecommunication requirements?
2. What practices/policies does the Component use to validate telecommunications requirements?
3. Does the Component have any plans to upgrade, improve, or implement a local or wide area network, and if so what considerations have been made regarding use of existing DoD capabilities/assets?
4. What is the process and the criteria used to allocate funds for telecommunication requirements?
5. When, and what were the results, of the last review and revalidation (R&R) to assure effective and efficient use of telecommunication assets?
6. Does the Component place special emphasis on requirements being transferred onto a common-user system to ensure previously used dedicated circuits were disconnected?
7. Does the Component have policies and procedures for ensuring that determinations are made by the customer regarding

November 1992

whether a requirement is exempt under 10 U.S.C. 2315 (Warner Exemption)?

8. Does the Component have policies and procedures for ensuring that a lease versus purchase analysis is performed by the customer to determine the most cost-effective telecommunications services acquisition strategy?

9. What policies and procedures does the Component use to ensure the acquisition of equipment and services that will conform to the standards of FIPS 146 (GOSIP) and other DoD standards?

10. Does the Component follow Telecommunications Service Priority (TSP) System rules and procedures for the National Security and Emergency Preparedness (NS/EP) services? These rules and procedures are found in 47 U.S.C. 64, NCS Directive 3-1, "Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NSEP)", NCS Manual 3-1-1, "Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NSEP) Service User Manual", and DOA Circular 310-130-4, "Telecommunications Service Priority (TSP) System".

11. What actions or plans does the Component have to ensure critical telecommunications services are available when needed, and what technologies are involved (fault-tolerant, uninterruptible power, backup facilities, etc.)?

12. How is the Component maintaining a centralized data base that contains an inventory of base telecommunications equipment and services?

13. What are the Component's policies and procedures to ensure uneconomical contracts are terminated?

14. How does the Component track spare capacity on telecommunications systems, and how is it assured that spare capacity is used when new requirements are received?

The following questions should be asked only when addressing issues involving the Defense Information Systems Agency management activities:

15. What is the process for reviewing each telecommunication requirement in light of Warner exempt determinations?

16. What are the policies and procedures in place regarding the processing of FTS 2000 exemption requests to GSA?

17. What procedures have been established for implementing the policies on how long-haul telecommunications requirements will be satisfied, i.e., DoD common-user systems. FTS 2000, open market?

November 1992

18. How are long-haul telecommunications invoices being reconciled?

F. RECORDS MANAGEMENT

Components are required by DODD 5015.2, "Records Management Program," to ensure that adequate controls over the creation of Component records are established; that Component functions are adequately and properly documented; that operational recordings are kept to a minimum; and that the accumulation of unnecessary records is prevented.

1. Has the IM organization issued a directive establishing a records management program (36 CFR 1222.20(b)(3))? Does the program directive:
 - a. Define what a record is (44 USC 3301) and make the proper distinction between federal records, nonrecords, and personal papers (36 CFR 1222.34 and 36)?
 - b. Assign responsibilities to an office or offices to develop and implement a Component-wide records program (36 CFR 122 0. 30 (b) (1)) ?
 - c. Information on removal of nonrecord materials is covered in 36 CFR 1222.42. NARA has published a checklist of personal papers for departing officials, "Personal Papers of Executive Branch Officers: A Management Guide."
2. How does the IM organization ensure the following actions are taken:
 - a. Provide the proper safeguards for component records to include advising officials and employees of their responsibilities to guard against and report unlawful removal or destruction of records (44 USC 3105)?
 - b. Ensure that records managers are included in the strategic planning process (41 CFR 201-6.002(f)) and that records management requirements are considered before approving new or enhancing old electronic record systems (para. 8, FIRMR Bul. B-1, Jan. 30, 1991)?
 - c. Provide for the creation, maintenance, use, and disposition of electronic records (36 CFR Part 1234)?
 - d. Prescribe uniform files maintenance procedures for all records?
 - e. Provide for periodic review of records management practices within the Component?
 - f. Provide for the uniform disposition of all records to include obtaining National Archives & Records Administration (NARA) approval for new or changed disposition schedules? Does it specify which records are transferred to a Federal

November 1992

Records Center and which directly to the custody of NARA, and are the steps in this process clearly explained? Establish a training program in files maintenance and records disposition for all clerical and administrative personnel? When these activities are decentralized is there someone checking on the procedures being followed to ensure quality control of the paperwork?

3. Has a Records Liaison Officer been assigned responsibility for the development and implementation of the Component-wide program?
4. Has the Component conducted an inventory of Component records to determine the types and locations of files created in the normal course of Component business?
5. Is a comprehensive Component-wide files manual available that includes a classification scheme designed for Component program files?
6. Have standards for maintenance and disposition of ADP records been developed?
7. Has the Component encountered problems in identifying and retrieving needed information from federal record centers in a timely manner?
8. Has responsibility for the management of electronic records been assigned to a specific organization? Has this responsibility been delegated in a formal directive if not, how has responsibility been assigned?
9. Does the Component's management of electronic records include records management considerations (e.g., identification of record copies and development of procedures for records creation, indexing, retrieval, and disposition)? See NARA Instructional Guide Series on "Managing Electronic Record" and page E-1 which is an extract from a draft DoD Manual on records management.
10. Has the Component specified security standards for electronic records and the equipment and media upon which they are processed?
11. Are electronic recording systems reviewed periodically for conformance to established procedures, standards, and policies?

G. PXPORIS

Components are required to establish a Reports Management Program by DODD 7750.5, "Management and Control of Information Requirements".

1. Has the Component established a Reports Management Program,?
If so, has/have an Information Management Control Officer(s)

November 1992

(IMCO) been designated to manage Public-Use, Interagency and Internal reporting requirements?

2. Is the Component's information requirements control activity established under the Component's Senior IM official or designated representative?
3. How does the Component ensure that information collected from the public; i.e., individuals, businesses, other private institutions, and state and local governments, is minimal, accounted for, controlled and non-duplicative?
4. How does the Component review and submit its Information Collection Budget to Washington Headquarters Services (WHS)?
5. What is the Component's review process for the Internal Reports Program? What types of assessments are made to ensure that internal reports are non-duplicative, valid, accurate, and essential to the mission of the Component?
6. What is the Component's review process for assigning, and canceling Internal Report Control Symbols (RCSS) for information collected from within their Component?
7. How does the component submit requests for approval of public-use and interagency information requirements to WHS?
8. How often does the Component conduct reviews of its internal and/or interagency reporting requirements? When was the last review accomplished?

H. FORMS MANAGEMENT

Components are required to have a Forms Management Program by DODD 77-110.7, "DoD Forms Management Program".

1. Does the Component have a Forms Management Program? If so, list the measures that have been implemented to prevent the proliferation of counterfeit or "bootleg" forms. Specify the measures taken for hardcopy and electronic forms.
2. Describe, in detail, the accountability practices the Component uses to design, print, ship, and stock accountable and safeguard forms.
3. Does the Component use identical internal and external coordination and concurrence procedures to process electronic and hardcopy forms? If not, describe how and why these procedures differ.
4. List the procedures the Component uses to prevent the unnecessary duplication of existing sub-Component and Component-wide forms.
5. Describe existing forms design training procedures and/or practices the Component uses.

November 1992

6. How does the Component ensure it is processing new and revised forms according to guidelines in existing DoD Forms Management Publications?
7. Does the Component require a current prescribing directive for each form in its Component Forms Inventory? If not, why not?
8. Describe the Component's procedures used to evaluate forms-related suggestions.

I. MAIL MANAGEMENT

The DoD Official Mail Program is contained in DoD 4525.8-M (DoD Official Mail Manual), dated July 1987. The Manual has had two changes. The object of the DoD Official Mail Program is to achieve cost-effective mail processing and transportation (postage) through proper use of the United States Postal Service.

1. How has the Component implemented the DoD Official Mail Program as guided by DoD 4525.8-M?
2. Are official mail managers assigned per DoD 4525.8-M, Chapter 2, subsection C.1.?
3. How is the Component implementing the training required by DoD 4525.8-M, Chapter 2, Subsection C.2.?
4. How is the Component implementing the supervision requirements in DoD 4525.8-M, Chapter 2, Subsection C.3.?
5. How is the Component implementing the inspection requirements in DoD 4525.8-M, Chapter 2, Subsection C.4.?
6. The DoD policy requiring decentralization of budgeting and payment for postage to the level where postage is obtained from the post office is intended to make users accountable for their use of postage. How has the Component implemented this policy and how has effective implementation been ensured?
7. How is the Component effectively implementing the DoD policy requiring the renumbering of buildings to street address format and the assignment of ZIP + 4 codes?
8. Is DoD 4525.8-M available at all postage metering locations as required by DoD 4525.8-M, Chapter 1, Subsection D.9.?

J. INFORMATION SYSTEMS SECURITY

Information is a valuable asset and, as such, should be safeguarded at all times against modification, tampering, loss, or destruction. The information system resource safeguards and procedures are necessary to ensure access is only by authorized people, resource usage is for intended purposes, and that data

November 1992

integrity is maintained. Such measures will ensure information integrity, availability, accountability, and confidentiality. DODD 5200.28, "Security Requirements for Automated Data Processing (ADP) Systems," and DoD 5200.28-M, "ADP Security Manual," stress the importance of a life-cycle management approach to implementing computer security requirements. Also, DODI 7920.5, "Management of End User Computing " states it is DoD policy to enforce the licensing provisions of commercial software and DoD 7740.1-G, "ADP Internal Control Guidelines," stresses the need for control procedures to ensure the proper management and use of computers.

1. How has the Component implemented security policies, directives, and guidance been developed or have existing procedures been modified to meet the requirements of the Computer Security Act of 1987?
2. What procedures are used to ensure that adequate security is provided for all automated systems?
3. What procedures are in place to ensure only those with a need-to-know have access to automated information systems (AISs)?
4. What AIS safeguards or procedures have been established for Protecting personal privacy information
5. What AIS safeguards or procedures have been established to ensure AIS integrity and the related information/system telecommunication resource availability is maintained?
6. Have training programs been established to ensure employee security awareness and use of accepted security practices
7. What Component LCM guidance exist on how security and privacy requirements are to be addressed when AIS and federal information processing resources are being acquired? When multiple AISs interface and exchange data?
8. What Component policies and procedures exist regarding the acquisition and use of federal information processing (FIP) resources that prohibit the use of copyrighted software that the Component has not leased or purchased? What disciplinary actions are taken when there is unauthorized use of copyrighted software?
9. How does the Component insure that all personnel are aware of copyrighted computer software licensing agreements and the potential consequences for copyright infringement.
10. What Component controls exist to insure that proof of legal possession of copyrighted computer software is retained for as long as the software is used? How does the Component identify the copyrighted computer software that is authorized to be installed on each computer?

K. APR/DPA MANAGEMENT

The solicitation is the formal method of conveying the government's requirements and forms the basis of award. It is essential that the solicitation identify government needs clearly, completely and accurately; provide evaluation factors; and specify applicable federal telecommunications standards (FED-STDS) and Federal Information Processing Standards (FIPS), and comply with the FAR and the FIRMR. The solicitation should indicate whether each standard is either applicable; not applicable; or applicable but waived. A delegation of procurement authority (DPA) from GSA places greater responsibilities on the Component to ensure compliance with FIRMR requirements. DODD 7740.1 requires each Component to designate a senior official or representative to be responsible for carrying out the Component's IM functions, including responsibility for acquisitions of FIP resources made pursuant to a DPA. When requesting a specific acquisition DPA, the Component certifies that required FIRM-N acquisition documentation has been or will be completed.

1. Has the Component designated an official to OSD or GSA who is accountable and responsible for acquisitions conducted under a DPA from GSA?
2. Does the Component maintain a tracking system that indicates the status of DPAs (e.g., expiration date, contract award information, and compliance with DPA conditions, including dollar limitations) and/or planned acquisitions for information resources?
3. What monitoring process exists to assure DPA constraints and conditions are followed?
4. Does an independent organization, other than OSD, review and approve acquisition documentation and required studies?
5. Does the contracting office have a copy of all AFRS, DPAS, and DPA Amendments on file?
6. Does the Component have policies and procedures for contractor performance validation? Who is responsible for conducting these validations and how frequently are they conducted?

Requirements Analysis

7. How does the Component ensure an appropriate requirements analysis is conducted when required?
8. How does the Component ensure the methods selected for documenting requirements are consistent with Component and DoD life-cycle management guidance?

November 1992

Analysis of Alternatives

9. How does the Component ensure that an appropriate analysis of alternatives has been conducted when required?
10. Are methods selected for analysis of alternatives based on DOD Component and DOD life-cycle management guidance?

Compliance with Applicable FIRMR Provisions Regarding Standards

11. Does the Component have an organizational structure to manage, control, implement, and ensure compliance with FED-STDS and FIPS PUBS?
12. Does the Component have a procedure in place for determining whether FIP standards should be waived and for how to request approval of a FIP standards waiver? (Note: Per Secretary of Defense memorandum dated February 18, 1992, only the DOD senior information management official and the senior information management officials of the Army, Navy, and Air Force may approve waivers to FIP standards.)

Conversion Study

13. How does the Component ensure conversion studies are conducted when required?
14. How does the Component ensure that the following costs are not included in the determination of conversion costs:
 - a. Conversion of existing software and data bases that would be redesigned regardless of whether or not augmentation or replacement FIP resources are acquired,
 - b. Purging duplicate or obsolete software, data bases and files,
 - c. Development of documentation for existing application software, and
 - d. Improvements in management and operating procedures?
15. How does the Component ensure that a conversion study is commensurate with the size and complexity of the requirement and the study includes any cost of conversion that can be stated in dollars as well as other expenses that are related to the conversion?

Support for Requirements Acquired Under Other than Full and open Competition

16. How does the Component ensure that there is proper justification for the use of other than full and open competition or specific make and model specifications?

November 1992

17. How does the Component ensure that actions are taken to foster competition in future acquisitions?

L. OVERSIGHT/DELEGATION OF AUTHORITY

Component oversight of information resources management and acquisition is a primary factor used in GSA's determination for granting specific and blanket delegations of procurement authority to agencies and will be a prime factor used by OSD and Components.

1. How does the Component ensure that individuals responsible for the management and acquisition of FIP resources comply with the FIRMR and DoD directives and instructions that implement the FIRMR?
2. Is there an organization that independently reviews all major acquisition requests and IM initiatives?
3. If the IM Organization has delegated some level of procurement authority, how do they oversee this delegation of authority?

M. EFFECTIVE CONTRACT ADMINISTRATION

A critical element of a Component's acquisition system is maintenance of an effective contract administration function to ensure contractor performance in accordance with the contract terms and conditions. An increasing concern of Congress, GSA, and the vendor community is the expansion of awarded FIP resource contracts to new users without proper authority and without complying with applicable acquisition regulations and contract law.

1. Does the Component have regulations and procedures in place for how contract administration assignments are to be made?
2. How does the Component ensure there is planning for how contract administration will be performed before contract award occurs?
3. Are contract administration assignments formally made? if not how are they made?
4. How does the Component ensure that contract modifications and change orders do not improperly exceed the scope of the contract or violate the conditions of the DPA?

N. REVIEW OF SELECTED CONTRACT FILES

Component acquisition management processes should ensure that FIP resource acquisitions meet competition requirements and comply with regulations. Several contract files, for different types of acquisitions (including acquisitions under GSA schedule contracts), should be selected and reviewed to demonstrate whether the Component is complying with FIRMR requirements.

November 1992

Files reviewed should include those that required a specific DPA as well as lower dollar value acquisitions that are within the agency's blanket regulatory DPA threshold. The reviews of these files should include the following:

1. Are all of the documents that were certified as complete in the APR (if required) available in the contract file, and were they completed as certified in the APR?
2. If a conversion study was not conducted, does the acquisition fall within one of the following FIRMR exceptions for a conversion study:
 - a. An initial acquisition where no FIP resources exist,
 - b. FIP equipment peripherals only, or
 - c. The exercise of a purchase option under a leasing agreement?

(Note: Per the FIRMR the above are the only valid reasons not to conduct a conversion study.)

3. Was the conversion study commensurate with the size and complexity of the requirement?
4. If the contract was awarded under other than full and open competition--
 - a. Does the contract file contain a fully approved "justification for other than full and open competition?"
 - b. Does the contract file clearly indicate actions taken or planned to foster future competition?
5. If the contract was for a compatibility-limited requirement does the contract file include a justification for use of a compatibility-limited requirement that is based on at least one of the following reasons:
 - a. The Component has technical or operational requirements for compatibility and the Component determines that replacing additional portions of the installed base to avoid compatibility-limited requirements is not advantageous to the government;
 - b. The Component determines that the risk and impact of a conversion failure on Component critical mission needs would be so great that acquiring non-compatible resources is not a feasible alternative?

(Note: Per FIRMR 201-20.103-4, a compatibility-limited requirement must be justified based on one of the above reasons.)

November 1992

6. A sufficient sample of orders under GSA schedule contracts should be reviewed and the following questions should be answered regarding each file to understand how the GSA schedule orders are managed:
 - a. Was a determination of need made and a requirements analysis conducted?
 - b. Was a system life established?
 - c. Was an analysis of alternatives conducted?
 - d. Was a conversion study conducted, if applicable?
 - e. If the requirement was restricted to one of the following, was a justification for a restrictive requirement prepared:
 - ** All or none
 - ** Only new
 - ** Specific made and model Other:
 - f. Was a pre-Commerce Business Daily (CBD) cost analysis conducted (i.e., comparison with other schedule contracts)?
 - g. Was the proposed schedule order synopsis in the CBD? If not, was the order less than \$50,000.
 - h. Did the CBD synopsis comply with the FIRMR 201-39.501-3?
 - i. Was an analysis performed to determine that the selected schedule contract represented the lowest overall cost?
 - j. was the schedule order within the maximum order limitation of the schedule contract?

O. COMPONENT IRM REVIEW PROGRAM

The Component's IRM oversight program creates a framework for performing several types of reviews and monitoring activities as they are applied to the Component's IRM and procurement management activities. These reviews include IPM reviews, reviews of major information systems, computer security reviews, management reviews, reviews of APRs and procurement management activities and processes. DODD 7920.1, "Life-Cycle Management (LCM) of Automated Information Systems (AIS)," provides guidance for AIS projects and activities concerned with the design, development, deployment, and operation of AISS. DoD Instruction 7740.3, "Information Resources Management (IRM) Review Program," requires Components to establish an IRM review program, and Components are asked annually to report on their review activities completed during the year and those planned for the

November 1992

next year. Component annual reports on completed IRM reviews should be reviewed before beginning the work below.

1. What are the number, skill level, and grade level of staff committed to the Component IRM review function?
2. What evidence is there of senior management commitment to the program?
3. How has the Component ensured compliance with Section 3506? Areas of concern include: inventory of major systems, review of IM activities, conduct of and accountability for acquisitions, implementation of governmentwide and Component information policies, principles, standards, and guidelines for information collection and reduction, statistical activities, records management, privacy and security of records, sharing and dissemination of information, acquisition and use of information technology? See Section 3506 on page A-1 for more detail.
4. Has the Component followed up on the recommendations and initiatives and actions that were identified in its completed IRM reviews? (A representative sample of IRM review reports should be reviewed, and the Component should be required to demonstrate that actions have been taken to implement the review findings. See page C-1 for list of common problems found by GSA.)

P. COMPUTER ACCESS BY USERS WITH DISABILITIES

GSA and the Department of Education have jointly developed procurement guidelines in consultation with the National Institute of Disability and Rehabilitation Research. These guidelines, published in October 1987, prescribe management responsibilities and functional performance specifications for the disabled end-user. Section 508 of the Rehabilitation Act of 1973, as amended, requires electronic office equipment purchased or leased by the federal government to be usable by people with disabilities. The General Services Administration has issued guidance in the Federal Information Resources Management Regulations and has published a handbook entitled "Managing End User Computing for Users with Disabilities." The Department of Defense has established a Computer/Electronic Accommodations Program (CAP) that provides funding and other types of assistance for all Components. The Assistant Secretary of Defense (Force Management and Personnel) has asked each Component to name a coordinator for access issues, and these coordinators meet periodically. See page D-1 for a list of pertinent references.

1. What has been the Component's contact with CAP? When has the Component had the CAP briefing? Have computer resources been acquired through the CAP office?
2. What steps has the Component taken to identify end users with disabilities and their needs, and to ensure that these

REQUIREMENTS OF SECTION 3506 OF THE PAPERWORK REDUCTION ACT

Each agency shall

- Carry out its information management activities in an efficient, effective, and economical manner, and comply with the information policies, principles, standards, and guidelines prescribed by the Director of ONM;
- Designate a senior official, reporting directly to the agency head, to carry out the responsibilities of the Act;
- Systematically inventory its major information systems and periodically review its MM activities;
- Ensure that its information systems do not overlap each other or duplicate the systems of other agencies;
- Each agency shall assess the reporting burden of proposed legislation;
- Assign to the official designated under [the Paperwork Reduction Act] the responsibility for the conduct of and accountability for any acquisitions made pursuant to a delegation of authority [under the Brook's Act];
- Ensure information collection requests required by law or to obtain benefit, and submitted to nine or fewer persons, contain a statement to inform the person receiving the request that the request is not subject to the requirements of section 3507 of the Paperwork Reduction Act;
- Implement applicable governmentwide and agency information policies, principles, standards, and guidelines with respect to information collection, paperwork reduction, records management activities, privacy and security of records, sharing and dissemination of information, acquisition and use of information technology, and other information resource management functions;
- Periodically evaluate and as needed, improve the accuracy, completeness, and reliability of data and records contained within federal information systems;
- Develop and annually revise a 5-year plan, in accordance with appropriate guidance provided by [OMB], for meeting the agency's information technology needs;
- Establish such procedures as necessary to ensure the compliance of the agency with the requirements of the Federal Information Locator System (Section 3506), including necessary screening and compliance activities.

ACTIVITIES
for
OSD-LEVEL IRM ASSESSMENTS

IRM COMPLIANCE REVIEWS

- DEFENSE ADVANCED RESEARCH PROJECTS AGENCY
- DEFENSE INFORMATION SYSTEMS AGENCY
- DEFENSE MAPPING AGENCY
- DEFENSE NUCLEAR AGENCY
- DEFENSE INVESTIGATIVE SERVICE
- DEFENSE FINANCE AND ACCOUNTING SERVICE
- WASHINGTON HEADQUARTERS SERVICE
- DEFENSE MEDICAL SUPPORT ACTIVITY
- DEFENSE CONTRACT AUDIT AGENCY
- DEFENSE COMMISSARY AGENCY
- AMERICAN FORCE INFORMATION SERVICE
- DEPARTMENT OF DEFENSE DEPENDENT SCHOOLS
- DEFENSE LOGISTICS AGENCY
- DEFENSE TECHNOLOGY SECURITY ADMINISTRATION
- DEPARTMENT OF DEFENSE INSPECTOR GENERAL

IRM REVIEW PROGRAM EFFECTIVENESS EVALUATIONS

- ARMY
- NAVY
- AIR FORCE

GSA IDENTIFIED IR/PMR PROBLEMS

IRM ORGANIZATION/PLANNING:

- Directives outdated
- Organizational changes made to fix past problems
- Records management function not under senior official
- More senior management involvement needed in IRM planning process
- Staffing not adequate
- Lack of formal and cohesive ERM organization
- IRM Council inactive for a year
- Insufficient resources on computer security management

ACQUISITION MANAGEMENT:

- No post-procurement oversight review program
- Broad authorities delegated to operational organizations without adequate evaluation or being supported by adequate management controls and oversight
- Little promotion of consolidated ADP contracts
- Contract awarded with no GSA DPA as well as allowed to exceed delegation authority
- Lack of timely advanced procurement planning results in high level of noncompetitive procurements and schedule slippages

INFORMATION TECHNOLOGY MANAGEMENT:

- Too many outdated computers
- Inadequate inventory and update procedures
- No software life-cycle management standards or program for electronic recordkeeping
- Lack of handicapped accommodation program

Note: GSA identified problems are from reviews of both Civilian and Defense agencies,

GUIDANCE RELATED TO ELECTRONIC ACCESS
FOR PEOPLE WITH DISABILITIES

- 29 U.S.C. 791(b) Section 501(b) of the Rehabilitation Act of 1973, as amended, which requires affirmative action in federal employment of persons with disabilities.
- 29 CFR 1613.701-707 Prohibits iriation in federal employment against a quauied person with a disability and requires federal agencies to provide reasonable accommodation and eliminate architectural and other barriers for employees and applicants with disabilities.
- EEO-MD-712 EEOC requirement, for comprehensive affirmative action programs for people with disabilities to be established by federal agencies. Specifies program elements to be included.
- DoD Directive 1440.1 Establishes the DoD Handicapped Individuals Program on the basis of various laws and regulations related to EEO/work Force diversity.
- 29 U.S.C. 794a Section 504 of the Rehabilitation Act of 1973, as amended, which prohibits discrimination programs and activities assisted or conducted by the federal government.
- DoD Directive 1020.1 Implements Section 504 for DoD.
- 40 U.S.C. 762 Telecommunications Accessibility Enhancement Act of 1988, which requires that the federal telecommunications system be made usable by people with hearing and speech impairments, including those who are federal employees.
- 29 U.S.C. 794d Section 508 of the Rehabilitation Act of 1973, as amended, which requires that computers and other electronic office equipment purchased or leased by the federal government be made accessible to persons with disabilities, including federal employees.
- 41 CFR 201 Federal Information Resources Management Regulation amendment on electronic accessibility implementing 29 U.S.C. 794d and 40 U.S.C. 762.
201-1.002-1 policy
201-17.001 Q) and (k) electronic access
201-18 (e) budget
201-18.002 (c) policy
201-20.103-7 acquisitions
201-3.402 deviations for accommodations

- FIRMR Bulletin C-8 Information accessibility for persons with hearing and speech impairments.
- Bulletin C-10 Telecommunications accessibility for persons with hearing and speech impairments.
- GSA Order ADM 5420.71A Establishes the Council on Accessible Technology (formerly Interagency Committee for Computer Support of Handicapped Employees), of which DoD is a member, to promote the productivity and achievement of federal employees with disabilities by making information technology accessible in the work place.

Electronic Records

A. Definition. Electronic records are those stored in a form that only a computer can process such as magnetic tapes, disks, drums, video files, and optical disks. There are two broad categories of electronic records:

1. Records generated in a central ADP facility. These are created or used by data input personnel, computer operators, programmers, analysts, and systems administrators.

a. They may include files required to manage system housekeeping, performance tuning, system usage, log-in and password control, and audit trail files.

b. All files included in this category must be individually appraised for permanent or long-term value, particularly those data bases created for action officers and/or offices that may contain significant sets of statistical or analytical data not duplicated in paper records. Where an electronic file duplicates a paper one, the electronic version need not be retained as long as the hard copy, but it must be included in the records schedule.

c. Originators of electronic data systems must ensure that adequate and up-to-date technical documentation for each system is maintained. The minimum required is a narrative description of the system; physical and technical characteristics of the records, including a record layout that describes each field including its name, size, starting or relative position, and a description of the form of the data (alphabetic, zoned decimal, packed decimal, or numeric), or a data dictionary or the equivalent information associated with a data base management system including a description of the relationship between data elements in data bases; and any other technical information needed to read or process the records.

d. Users must also furnish the information required by the National Archives when submitting a new electronic record file for approval. This information is provided to the NARA on NA Form 14028, "Information System Description", as an attachment to SF 115, "Request for Records Disposition Authority". SF 115 is prepared by the Records Management Division and forwarded to the National Archives. Copies of NA Form 14028 are available from the Records Management Division. The following information is required:

(1) Name of the system. Use the commonly used name and acronym of the system.

(2) System control number. Specify the internal control number assigned for reference, control, or

cataloging purposes.

(3) Agency program supported by the system.

(4) Purpose of the system. Indicate the reasons for the system and the requirements met by it.

(5) Data input and sources. Describe the primary data input sources and the providers of the data to the system.

(6) Major output. Show the system's main products and the frequency of their preparation. Also state whether the information is transferred to other systems.

(7) Information content. Describe the main subject matter, date coverage, time span, geographic coverage, update cycle, and other major characteristics. Also state whether it saves superseded information and whether it contains microdata or summary data. Indicate the location of documentation needed to read and understand the files and list any restrictions on their access and use, national security, privacy, or other.

2. Records created in an office setting.

a. Examples are word processing, spreadsheet, and database files; electronic mail and message files; electronic calendars; appointment, telephone, trip and visit logs; finding or tracking aids, and other "helpers" employed to enhance the effectiveness of the system. When these electronic files are used strictly as backup for paper record copies, or they contain only transitory information that does not document the activities of an office, the appropriate General Records Schedule (GRS) series for disposable electronic records will be used. The electronic file may be erased when the hard copy has been generated or when the data is no longer needed. However, users may elect not to erase certain electronic files, particularly if they are reusable for later revision of manuals, directives, recurring memoranda, and spreadsheet models.

b. An office that relies only on electronic versions of files for any of its official records must appraise and schedule them. Some components may have a "hybrid" system; e.g., BOTH paper and electronic versions of their official records. Offices purchasing new systems or upgrading old ones must ensure that records disposition instructions for the data are incorporated into the system's design.

B. General. When electronic records meet the criteria established for Federal records -- information made or received in connection with the transaction of public business and

appropriate for preservation as evidence of an agency's organization, functions, policies, etc., or because of their informational value -- those who create and use them must ensure their proper disposition, as for paper records, where the originator or user, in coordination with the OSD Records Administrator, designs a disposition schedule which is approved by the Archivist of the United States.

1. Mission-related data bases, as distinct from those purely administrative files described in a GRS, must be scheduled as long-term or permanent records. Records officers must pay particular attention to data bases that contain significant statistical data or information related to policy-making functions and schedule them.

2. The management of electronic records is the same as that for paper records: Files needed often for the conduct of business should be stored conveniently for immediate access. Those less frequently needed should be stored on tape, disk, or other media, for retrieval when required. Files not requiring long-term retention or not needed to document the business of an organization, such as draft versions of documents, should be deleted from the storage media in accordance with the appropriate disposition schedules. Classified information should be deleted in accordance with DoD Regulation 5200.1-R.

C. Electronic Recordkeeping Systems. An example of an electronic recordkeeping system in a "paperless office" is one where the original records are generated by a word processor or a personal computer and stored on a magnetic disk. While paper copies are printed for distribution, the official record copies are retained on a mass storage device. After a specified period of time they are erased or transferred to a magnetic tape for eventual transmittal directly to the NARA for permanent retention.

a. Electronic records are not forwarded to a Federal Records Center for retention or disposal, because the FRCs do not have specialized maintenance equipment to ensure the retention of data on magnetic tape for permanent files. Temporary electronic records are not stored in the Federal Records Centers.

b. The key to determining the retention of any record, electronic or paper, is its value to its creator. When information exists in both machine-readable and hard-copy formats, including computer output microform (COM), various factors bear on deciding which medium should be retained for archival purposes. Among these are the relative costs of storage and preservation, the relative convenience of reference, and the facility with which most hard-copy documents may be regenerated from machine-readable files.

D. Managing Electronic Records. In practice, there is no difference between managing electronic and paper records.

1. The contents of the computer's directory or the sum of all electronic "folders" equates to the traditional file drawer; each computer data subdirectory or electronic "folder" is the equivalent of a paper file folder; files in directories or "folders" are individual "documents" in the folder. Directory or "folder" names are like file folder labels in that they identify the broad functional category of the information contained in them; file names are like the filing instructions written on papers before they are put away.

2. Each document contained in electronic form must be identified sufficiently to enable-authorized personnel to retrieve, protect, and carry out its disposition.

E. Filenaming Conventions.

1. Naming electronic files resembles labeling paper file folders except for two important differences:

a. Most computer operating systems limit the length of a filename, in some instances to a total of eleven characters (eight for a name with three as an extension); others permit 25-30 characters, allowing more descriptive file naming.

b. The other difference is that conventions for file naming are not standardized even in offices with good records management programs. It is essential that file-naming conventions be standardized.

2. Software programs that can locate a particular file by searching for a text string are also available. This capability is incorporated in some word processing programs or is available as a separate utility program.

F. Labels. Identification of electronic records is accomplished at two levels:

1. External. Actual labels affixed to individual diskettes and tapes. To prevent damage to the medium, records information should be written or typed before the label is affixed; never erase information on a label once it is in place. When affixing a label to a disk, choose an area away from all holes. Be sure labels identify the hardware and software that will read the information stored on the medium. Labels should contain the same information required on paper file folder labels: Security classification (if applicable), file series designation, description, and disposition instructions.

2. Internal. Electronic labels located in subdirectories

or "folders" provide sufficient information to find files on hard disks, floppies, magnetic tape, etc. The file series designations that appear in an agency's disposition manual should also be used to name subdirectories. For example, a subdirectory which might be labeled 70202PD.2 and called Community Relations Programs Division files containing correspondence on arrangements for briefings, conferences, tours, etc., that are destroyed after 3 years. Any logical combination of alphanumeric characters permitted by the operating system and descriptive of the series is suggested in naming subdirectories or folders".

Computer Directory Showing Office Subdirectories

C:\	C:\WP
(ro-t)	(program)
	:\WP\70202PD.2 (Co=. Relations)
	:\WP\7 0 2 02 PD. 3
	:\WP\70202PD.4

G. Guarding Against Data I4ss.

I. The best defense against lost data is making frequent backup copies of files. Data files should be backed up onto floppy disks or tapes after each change or update, but at a minimum backups should be done weekly. Magnetic tape is preferable for storage of backup material because floppy diskettes are more vulnerable to mishandling, and loss of data is common with this redi=-. When diskettes are the only backup medium available, they may be used for temporary storage of both permanent and temporary records. If possible, the backup media should be stored in a separate area from the source data to provide additional insurance against data loss.

2. Additional causes of data loss are equipment failure and power outages. In central processing facilities and minicomputer sites, as well as offices supported by local area networks, system failures are a relatively common occurrence. Users should save files frequently. A program feature that permits a user to save a file without exiting can be a very useful hedge against data loss when the equipment goes down.

3. When a system failure is caused by a power supply problem, data loss may be eliminated or minimized by the use of Uninterruptible Power Supply (UPS) equipment.' UPS equipment provides temporary emergency power to a system, allowing operator personnel time to alert users to save and close files and to permit bringing a computer system down with virtually no loss of user data. A good standby-power supply with filtration and surge suppression is recommended in multi-user computer environments

where there is danger of data loss because of an unreliable power source.

4. Single-user computers and individual workstations can obtain some protection against voltage spikes, overvoltages and surges with relatively inexpensive "surge protector" devices. These protect against some of the problems encountered when using commercial AC power, but not against sags, brownouts, and blackouts, which comprise most of the problems. Although protectors can lengthen the life of computer components, they are of no help under low or no-voltage conditions. Saving data frequently and making backups remains the best way to guard against data loss. Users are also cautioned about inexpensive surge protectors which deteriorate over time, making it virtually impossible to detect when they are no longer effective. Whenever possible, users should replace inexpensive ones with unlimited life induction coil surge protectors.

E. Optical Discs. This technology is having a revolutionary impact on the storage and retrieval of large quantities of information, and its acquisition is encouraged wherever its use proves cost effective. However, because Optical Disk (OD) systems are hardware- and software-dependent and since standards have not yet been developed to ensure transfer of data from one system to another, the National Archives CANNOT presently accession FE NT records stored on ODs.

1. OD technology may be used for all records authorized for disposal in the current files area, consistent with the lifespan of the disk medium itself.

2. Permanent records may be stored on ODs while retained by the originating agency. However, they must be converted to a medium acceptable to the NARA either when entered into the system or when transferred to NARA's legal custody. At the present time, acceptable media are hardcopy paper and one-half inch reel-to-reel or 3480 class c @ ridge magnetic tape.

3. Analog videodiscs that typically contain photographs are one type of optical disk that can be accessioned by the NARA providing no interactive software or nonstandard equipment is required to read them. Original photographs appraised as permanent and copied onto a videodisc must be scheduled for transfer to the NARA together with a copy of the videodisc. Likewise, compact disks used for digital audio playback may be transferred because they use a standard player and require no special software to use.

1. Acquisition and Upgrading-of Systems. Any office contemplating the acquisition of systems or upgrading existing ones should contact their agency records officer for guidance in this area.