NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

RIN 3095–ZA04

General Records Schedule 24, Information Technology Operations and Management Records; Request for Comments

AGENCY: National Archives and Records Administration.

ACTION: Notice of proposed records schedule; request for comments.

SUMMARY: As required by statute (44 U.S.C. 3303a(d)), the National Archives and Records Administration (NARA) issues General Records Schedules (GRS) to provide disposal authority for temporary administrative records common to several or all agencies of the Federal Government. The GRS include records relating to civilian personnel, fiscal accounting, procurement, communications, printing, and other common functions. NARA has developed a new General Records Schedule, Information Technology Operations and Management Records, to provide disposal authority for certain administrative records generated in or acquired by agency components responsible for developing and operating network infrastructure and systems.

NARA invites public comments on this proposed new general records schedule, as required by 44 U.S.C. 3303a(a). Because of the widespread interest in the management of electronic records, NARA is publishing the full text of the schedule with additional information on each item.

DATES: Comments must be received in writing on or before August 26, 2002.

ADDRESSES: Comments should be sent to Modern Records Programs (NWM), National Archives at College Park, 8601 Adelphi Road, College Park, MD 20740–6001, faxed to 301–837–3697 or 301–837–3698, or sent to the following Internet address: *records.mgt@nara.gov.*

FOR FURTHER INFORMATION CONTACT: Michael L. Miller, Director, Modern Records Programs, 301–837–1980.

SUPPLEMENTARY INFORMATION: In 1978, use of the GRS was made legally mandatory. A Federal agency must destroy records in accordance with the GRS to the greatest extent possible. If an agency wishes to apply a different retention period for any series of records included in the GRS, the records officer must submit a Standard Form (SF) 115 providing justification for the desired deviation.

Relationship of This Draft GRS to GRS 20, Electronic Records

This schedule does not duplicate or replace GRS 20, Electronic Records. The proposed new schedule addresses the administrative records generated by units responsible for technical management of IT resources. The functions covered by the proposed GRS 24 are comparable to the administrative functions relating to budgeting, contracting, human resources, and property management that are covered by other GRS. The proposed GRS 24 does not apply to system data or information content, which must be scheduled separately by submitting an SF 115, Request for Records Disposition Authority, to NARA.

GRS 20 remains in effect to cover the records described in that schedule. GRS 20 records include certain files associated with temporary data base management systems such as print files, extract files, source records, and certain disposable electronic records produced by end users in office automation applications. NARA will conduct a separate review concerning the continuation of GRS 20 disposition authorities as part of its comprehensive review of the policies and procedures for scheduling and appraisal of records in all formats.

Background—Development of This Draft GRS

In late 1997, the Archivist established an interagency Electronic Records Work Group to review General Records Schedule 20 and recommend revisions to that schedule or other practical solutions for the scheduling of electronic records. In 1998, the work group submitted its final report to the Archivist (*http://www.nara.gov/records/grs20/reprt914.html*) recommending, among other things, that NARA issue a new general records schedule for information technology operations and management records to supplement, not replace, GRS 20.

Building on the efforts of the Work Group, NARA drafted a new GRS for common administrative records relating to operation and management of information technology and related services. Federal agencies reviewed the draft in the summer of 1999. The draft, revised in response to agency comments, was discussed at a January 2000 focus group meeting with agency records management and information technology management officials. NARA made appropriate changes in response to comments made at the meeting and in June 2000 again requested comments from Federal agencies.

Overall, agencies found that the schedule draft they reviewed in 2000 generally fits their records and could be implemented without undue difficulty. In response to specific comments about terminology, apparent redundancies, and retention periods for some items, NARA consolidated some items and provided other clarifications to address the concerns. NARA believes the schedule is now at the appropriate level of detail. Given the agencies' interest in having more flexibility in applying disposition standards for temporary records, NARA eliminated the cutoff instructions and reworded some of the disposition instructions to allow agencies disposition options based on their internal procedures and operations. NARA clarified that the schedule covers only the temporary administrative records described in the various items. It does not cover all records maintained by Information Technology (IT) management organizations. Agency responsibilities to schedule records documenting unique agency programs should now be more apparent.

On the advice of the Office of Management and Budget, in October 2001 NARA requested one last Federal agency review of this notice containing the proposed schedule and explanatory information for each item. This information includes the records appraisal analysis normally provided in a separate appraisal memorandum. Based on comments received in October, NARA made some changes for clarification and elimination of redundancies. Federal agencies should note that the disposition instructions for items 1a and b, 2, 9b, 12b, and 13b, and the description for items 1b, 3b, 4a and b, 6a and b, 9a and b, 12a, and 13 were modified in response to the comments on the October 2001 draft. In addition, former item 8b was incorporated into former item 9, and former items 8a and 11 were deleted. The remaining schedule items were renumbered accordingly.

Throughout the process of developing and refining this new GRS, NARA representatives consulted with agency records officers and IT officials to resolve questions and clarify coverage of items. NARA analysts also reviewed records both within NARA and in a number of other agencies to ascertain the content of files. The information gathered during these consultations and examination of records is reflected in the appraisal analysis following each item.

Given the multiple reviews by Federal agencies, NARA believes that this schedule will be useful and relevant to

agencies. NARA now invites public comment on this proposed new General Records Schedule for Information Technology Operations and Management Records. Following is the complete text of the proposed GRS. The explanatory information and appraisal analysis is provided in brackets at the end of each item.

General Records Schedule 24—Information Technology Operations and Management Records

Introduction

This schedule provides disposal authorization for certain files created and maintained in the operation and management of information technology (IT) and related services. As defined in the Information Technology Management Reform Act of 1996 (now the Clinger-Cohen Act), ''information technology'' includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

This GRS does not cover all records relating to information technology operations and management. Offices with responsibility for IT operations also maintain administrative records covered by other GRS and records not in the GRS that must be scheduled by the agency. In addition, this GRS does not apply to system data or information content, which must be scheduled separately by submitting an SF 115, Request for Records Disposition Authority, to NARA.

The disposition instructions apply to records regardless of physical form or characteristics. Records may be maintained on paper, in microform, or electronically. Dispositions apply, however, only to records that are maintained as described in each item or subitem. If documents are part of a larger case file or recordkeeping system that contains records not covered in this GRS, agencies must separately schedule that file or system by submitting an SF 115 to NARA. If records covered by more than one item in this schedule are maintained together in one file or recordkeeping system, agencies must retain the records for the longest retention period authorized for those items.

Note that GRS 20, Electronic Records, remains in effect. GRS 20 covers certain temporary files associated with data base management. This new schedule supplements GRS 20 by providing disposal authority for temporary records relating to overall IT management, as opposed to the operation and use of specific systems. NARA is reviewing alternatives to GRS 20 and will develop revised requirements as it explores new approaches to managing electronic records.

1. Oversight and Compliance Files

Records in offices with agency-wide or bureau-wide responsibility for managing IT operations relating to compliance with IT policies, directives, and plans including recurring and special reports, responses to findings and recommendations, and reports of follow-up activities.

a. Performance measurements and benchmarks.

Destroy/delete when 5 years old or 1 year after responsible office determines that there are no unresolved issues, whichever is longer.

b. All other oversight and compliance records including:

- Certification and accreditation of equipment
- Quality assurance reviews and reports
- Reports on implementation of plans
- Compliance reviews
- Data measuring or estimating impact and compliance

Destroy/delete when 3 years old or 1 year after responsible office determines that there are no unresolved issues, whichever is longer.

[Note: See item 3b for performance files relating to systems.]

[*Appraisal analysis:* Item 1a covers such records as statistical performance data concerning system (and network) operations, including process steps or paths, time required for completion, and event or error indicators. These records include system availability reports that draw upon sample performance indicators to measure overall system performance. The retention period for this item relates to the ''5 year plans'' typically associated with IT systems.

Item 1b covers such materials as target IT architecture reports, systems development lifecycle handbooks, computer network assessments and follow-up documentation, authority to operate records, and certification and accreditation of equipment. These records are critical to the proper functioning of systems. Network assessments, for example, are conducted at regular intervals, and in cases where performance is found to be in need of improvement, the agency institutes a process to change or upgrade network equipment, configuration, or other components. Records under this item typically take the form of structured reports. Examples include contractor evaluation reports and other quality assurance records, market analyses and performance surveys, and benefit-cost analyses. Agencies may also maintain other compliance reviews including related analyses such as histograms illustrating trends across time for various groups, activities, and systems, and follow-up correspondence and corrective action reports.

The proposed dispositions for these will ensure the availability of records for a period of time that is sufficient to allow adequate systems management and will also ensure the preservation of records identifying problems until the problems have been resolved.]

2. IT Facility, Site Management, and Equipment Support Services Records.

Records maintained by offices responsible for the control and operation of buildings and rooms where IT equipment, systems, and storage media are located including:

- Files identifying IT facilities and sites, and
- Files concerning implementation of IT facility and site management and equipment support services provided to specific sites, including reviews, site visit reports, trouble reports, equipment service histories, reports of follow-up actions, and related correspondence.

Destroy/delete when 3 years old, or when superseded or obsolete, whichever is longer.

[*Appraisal analysis:* These records document the control and operation of buildings and rooms where IT equipment, systems, and storage media are located. Files include listings of facilities, trouble reports, reports on site visits and inspections, and service histories for equipment. Also included are copies of agency directives and lines of authority relating to such matters as facility operations, physical security of facilities, environmental security, including documents on fire prevention and control, electric power supply protection, magnetism protection, and ''good housekeeping'' procedures for protection against dust, dirt, and fire hazards.

These records need only to be kept for a relatively short period of time to satisfy administrative and operational needs. The proposed three-year retention period is adequate to ensure that IT operations are carried out in an environment that meets all applicable standards.

Records documenting control and operation of facilities that are maintained by units responsible for facilities management and physical security are retained for varying periods of time in accordance with other GRS items (e.g., GRS 18, items 9 and 10) and individual agency schedules.]

3. IT Asset and Configuration Management Files.

a. Inventories of IT assets, network circuits, and building or circuitry diagrams, including equipment control systems such as databases of barcodes affixed to IT physical assets. Destroy/delete 1 year after completion of the next inventory.

b. Records created and retained for asset management, performance and capacity management, system management, configuration and change management, and planning, follow-up, and impact assessment of operational networks and systems. Includes, but is not limited to:

(1) Data and detailed reports on implementation of systems, applications and modifications; application sizing, resource and demand management; documents identifying, requesting, and analyzing possible changes, authorizing changes, and documenting implementation of changes; documentation of software distribution and release or version management.

Destroy/delete 1 year after termination of system.

(2) Records of IT maintenance on the network infrastructure documenting preventative, corrective, adaptive and perfective (enhancement) maintenance actions, including requests for service, work orders, service histories, and related records.

Destroy/delete when 3 years old or 1 year after termination of system, whichever is sooner.

[*Appraisal analysis:* This item covers routine administrative records relating to existing IT systems, such as inventories of assets, including equipment control systems, databases of barcodes affixed to physical assets, work orders and service histories on maintenance of network infrastructure, and reports and other files relating to system implementation and modification. Detailed information is found in bar code reports, asset management guides, requests for services, requisitions for equipment, leases, change orders, purchase orders, property transfer control systems, flow reconfiguration requests, standardization requests and justifications. Other records include listings of devices such as routers, hubs, switches, and servers, described by make and model, location, and pertinent capacity and configuration information. These records differ from those covered by item 11. The records under item 3 relate to the ongoing maintenance and management of existing IT assets. The records under item 11 relate to the acquisition and implementation of new systems.

The proposed retention period in item 3a is appropriate since only current inventories are needed. Note that documents (or sections of documents) that are unchanged from prior inventories but that remain valid are kept in conjunction with current inventories. The proposed disposition instructions for item 3b(1) reflects the business need to retain for the life of a system detailed reports and data concerning the implementation, modification, and upgrading of systems infrastructure. For item 3b(2), the proposed disposition enables disposal of system maintenance records when three years old or one year after termination of the system, whichever is sooner. This will enable the agencies to ensure that proper maintenance procedures have been followed and to allow for any follow-up activities. If any maintenance activities have a major impact on a system, or lead to a significant change, those activities should be documented in item 3b(1).]

4. System Backups and Tape Library Records.

a.Backup tapes maintained for potential system restoration in the event of a system failure or other unintentional loss of data.

(1) Delete/destroy incremental backup tapes when superseded by a full backup, or when no longer needed for system restoration, whichever is later.

(2) Delete/destroy full backup tapes when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later.

[Note: See GRS 20, item 8, for backups of master files and databases.]

b. Tape library records including automated files and manual records used to control the location, maintenance, and disposition of magnetic media in a tape library including list of holdings and control logs.

Destroy/delete when superseded or obsolete.

[*Appraisal analysis:* This item pertains to records accumulated to ensure the ability to resume operations in the event of a system failure. Item 4a covers incremental and full system backup tapes maintained for potential system restoration. It is distinguished from GRS 20, item 8, Backups of Files, which covers security copies of the substantive contents of master files and databases. The GRS 24 item applies to an IT shop's backups of system software (which, due to system configuration, may also include substantive data separately covered under GRS 20, item 8). Item 4b applies to Tape Library records including automated files and manual records controlling location maintenance, and disposition in a tape library of the records covered by item 4a, including lists of holdings and control logs. These records include ''vault lists,'' and other reports listing all back-up medium, documents certifying the completion of backup processes, and other run tasks and differential backup activities. Tape libraries also maintain the addresses of offsite storage facilities, and ''bin'' location within storage facilities.

Agencies may produce backups for purposes other than system restoration. Master file and database backups, which are produced to ensure against the loss of documents and other data, remain covered by GRS 20, item 8, Backups of Files. Item 4a of this schedule pertains to backups implemented by systems administrators to ensure the ability to restore the entire system in the event of a major network failure.

The proposed GRS provides that incremental back-up tapes be destroyed when superseded or when no longer needed for system restoration. This disposition instruction allows agencies to keep only the current incremental backup or to retain it as long as the agency considers it may be needed for system restoration. Agencies will keep at least one additional backup of the full system, for security purposes. As for the incremental backups, agencies decide if the basic retention period is sufficient and may keep full backups for as long as they may be needed for system restoration. The disposition instruction for records used to control the location, maintenance, and disposition of magnetic media in a tape library provides for destruction when they are superseded, obsolete, or no longer needed. This authorization is appropriate because agencies need only the current, accurate information on the location and status of backup tapes.]

5. Files Related to Maintaining the Security of Systems and Data.

a. System Security Plans and Disaster Recovery Plans.

Destroy/delete 1 year after system is superseded.

b. Documents identifying IT risks and analyzing their impact, risk measurements and assessments, actions to mitigate risks, implementation of risk action plan, service test plans, test files and data.

Destroy/delete 1 year after system is superseded.

[*Appraisal analysis:* Item 5a provides disposal authority for records that outline official procedures for securing and maintaining IT infrastructure, typically system security plans, disaster recovery plans, and continuity of operations plans. The files include such records as published computer technical manuals and guides, examples and references used to produce guidelines covering security issues related to specific systems and equipment, records on disaster exercises and resulting evaluations, network vulnerability assessments, risk surveys, and other studies, such as formal security vulnerability assessments conducted by IG offices. These records relate to the specific systems for which they were written. System replacements will have new security and risk management requirements that may be totally different because of the architecture of the replacement system. The disposition instruction for item 5a provides for maintenance of the records to ensure a continuity of security controls throughout the life of the system.

Item 5b covers analysis of security policies, processes, and guidelines, as well as system risk management and vulnerability analyses. Examples of specific documents are automated information systems security directives and computer virus handbooks. Records covered by GRS 18, item 27 may appear similar, but GRS 18 relates to plans developed to protect life and property and GRS 24 covers records relating specifically to the security of IT systems. The retention period for these records reflects the need to retain records while a system is current and provides for review of documentation for superseded systems in connection with ensuring adequate protection for new systems.]

6. User Identification, Profiles, Authorizations, and Password Files

EXCLUDES records relating to electronic signatures.

a. Systems requiring special accountability, *e.g.,* those containing information that may be needed for audit or investigative purposes and those that contain classified records.

Destroy/delete inactive file 6 years after user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.

b. Routine systems, *i.e.,* those not covered by item 6a.

See GRS 20, item 1c.

[*Appraisal analysis:* Item 6a provides disposition instructions for user identification records, including user profiles and passwords associated with systems requiring special accountability, such as systems containing information that is security classified. The item authorizes the destruction of records concerning user identification six years after a user account is terminated or password is altered, or when it is no longer needed for security purposes, whichever is later. This will permit agencies to retain user identification records associated with highly sensitive or potentially vulnerable systems in order to provide historical data that may be needed in support of investigations or litigation arising from inappropriate access.

Records covered under item 6b include records such as user passwords and profiles for those systems not requiring special accountability. The records in these systems are typically system generated according to preset requirements. A system may, for example, prompt users for new passwords every 90 days for all users. These records are covered by GRS 20, Item 1c.]

7. Computer Security Incident Handling, Reporting and Follow-up Records

Destroy/delete 3 years after all necessary follow-up actions have been completed.

[*Appraisal analysis:* This item covers records relating to attempted or actual system security breaches, including break-ins (''hacks''), virus threats, improper staff usage, failure of security provisions or procedures, and potentially compromised information assets.

These records typically consist of narrative reports and background documentation relating to individual events or issues. These records include references to unauthorized intrusions, web site defacement, misuse of system resources, and other incidents noted by the Federal Computer Incident Response Center (FedCIRC, http://www.fedcirc.gov).

Retaining records for 3 years after all follow-up actions, including judicial procedures, have been completed ensures the availability of active case records and provides an adequate amount of time after a case is closed for any necessary follow-up action. Any significant incidents (e.g., a major system failure or compromise of critical government data) would be documented in program records, such as those in the office of the Inspector General, which must be scheduled separately by submitting an SF 115 to NARA.]

8. IT Operations Records

a. Workload schedules, run reports, and schedules of maintenance and support activities.

Destroy/delete when 1 year old.

b. Problem reports, proposals for changes and related decision documents relating to the software infrastructure of the network or system.

Destroy/delete 1 year after problem is resolved.

c. Reports on operations, including measures of benchmarks, performance indicators, and critical success factors, error and exception reporting, self-assessments, performance monitoring; and management reports.

Destroy/delete when 3 years old.

[*Appraisal analysis:* Item 8a includes workload schedules, run reports, including cycle time reports, schedules of maintenance, and related records. It is generally agreed within the Federal IT community that the value of these voluminous records expires after one year.

Item 8b covers problem reports, proposals for changes and related decision documents relating to the software infrastructure of a network or system. The retention period proposed for these records will satisfy the administrative and operational needs of IT offices by ensuring the retention of records relating to issues until they have been resolved.

Item 8c covers reports on operations, including measures of benchmarks, performance monitoring, and management reports. Agencies indicated that the proposed retention period would meet their administrative and operational requirements for these routine files.]

9. Financing of IT Resources and Services

Note: Copies of records needed to support contracts should be filed in procurement files, which are scheduled under GRS 3.]

a. Agreements formalizing performance criteria for quantity and quality of service, including definition of responsibilities, response times and volumes, charging, integrity guarantees, and non-disclosure agreements. Destroy/delete 3 years after agreement is superseded or terminated.

b. Files related to managing third-party services, including records that document control measures for reviewing and monitoring contracts and procedures for determining their effectiveness and compliance. Destroy/delete 3 years after control measures or procedures are superseded or terminated.

c. Records generated in IT management and service operations to identify and allocate charges and track payments for computer usage, data processing and other IT services EXCLUDING records that are part of the agency's cost accounting system, which are covered in GRS 8, items 6 and 7.

Destroy/delete records with no outstanding payment issues when 3 years old.

[*Appraisal analysis*: These records include agreements formalizing performance criteria for quantity and quality of service, files related to managing third-party services, and records generated in IT management and service operations, financial records including service level agreements defining service and support levels in quantified terms workload, hardware, software, as well as ad hoc reports documenting the continued validity of financial agreements. Records also include documentation related to contractor award fee for superior service.

These records relate to financial management, not IT equipment and services per se, and should be kept for three years after agreements, procedures, and payment issues are superseded, terminated, or resolved, as applicable. This retention period reflects normal audit cycles. These files are kept by IT offices to support their role in the acquisition of and payment for computer software and services. Records pertaining to these subjects that are needed to protect legal rights, address fiscal concerns, and/or provide Government accountability are maintained in procurement and finance offices in accordance with other GRS items or agency schedules.]

10. IT Customer Service Files

a. Records related to providing help desk information to customers, including pamphlets, responses to ''Frequently Asked Questions,'' and other documents prepared in advance to assist customers. Destroy/delete 1 year after record is superseded or obsolete.

b. Help desk logs and reports and other files related to customer query and problem response; query monitoring and clearance; and customer feedback records; and related trend analysis and reporting. Destroy/delete when 1 year old or when no longer needed for review and analysis, whichever is later.

[*Appraisal analysis*: The records covered by Item 10 relate to providing customer service and individual support to customers. Included are such records as pamphlets and Frequently Asked Questions, help desk logs and incident reports, ''help desk tickets,'' user guides, trouble reports, customer queries, feedback records, and trend analyses. These document end-user inquiries and requests for assistance.

These voluminous records are critical to the effective operation of IT systems. However, they have administrative value for only a brief period of time. This item will authorize destruction of customer service records such as pamphlets and lists of ''frequently asked questions'' (FAQs) one year after the record is superseded or obsolete and that help desk logs and other files related to customer query, feedback, and analysis be destroyed when one year old. The recommended disposition instructions will satisfy the administrative and operational needs of IT offices, including the need to dispose of these files in a timely fashion.]

11. *IT Infrastructure Design and Implementation Files*

Records of individual projects designed to provide and support new agency IT infrastructure (see Note), systems, and services. Includes records documenting:

- Requirements for and implementation of functions such as
  - —Maintaining network servers, desktop computers, and other hardware
  - —Installing and upgrading network operating systems and shared applications
  - —Providing data telecommunications
- Infrastructure development and maintenance such as
  - —Acceptance/accreditation of infrastructure components
  - —Analysis of component options, feasibility, costs and benefits
  - —Work associated with implementation, modification, and troubleshooting
- Models, diagrams, schematics, and technical documentation
- Quality assurance reviews and test plans, data, and results.

a. Records for projects that are not implemented. Destroy/delete 1 year after final decision is made.

b. Records for projects that are implemented.

Destroy/delete 5 years after project is terminated.

c. Installation and testing records. Destroy/delete 3 years after final decision on acceptance is made.

[Note: IT Infrastructure means the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Components include hardware such as printers, desktop computers, network and web servers, routers, hubs, and network cabling, as well as software such as operating systems (e.g., Microsoft Windows and Novell NetWare) and shared applications (e.g., electronic mail, word processing, and database programs). The services necessary to design, implement, test, validate, and maintain such components are also considered part of an agency's IT infrastructure. However, records relating to specific systems that support or document mission goals are not covered by this item and must be scheduled individually by the agency by submission of an SF 115 to NARA.]

[*Appraisal analysis*: These records pertain to individual new enterprise projects designed to provide and support agency IT infrastructure. IT infrastructure includes the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Included are hardware, software, and the services necessary to design, implement, and maintain such components. This item covers records concerning the infrastructure of IT operations. These records do not document programs fundamental to an agency's mission nor the IT systems utilized by agencies in carrying out their distinctive functions. Rather, these records are clearly administrative in nature and are of the same character throughout the Government. Records include developmental records such as quality assurance plans, requirement specifications, technology refresh plans, operational support and test plans, final operational support plan, and post installation reviews and briefings. These records differ from those found in Item 3 above. Item 3 is concerned with the ongoing maintenance and management of existing IT assets. Item 11 is concerned with the acquisition and implementation of new operating systems.

The disposition instruction for item 11a provides that records for projects that are not implemented be destroyed/deleted one year after a final decision has been made. This retention period is appropriate. If a proposed project is rejected, there is no need to retain the related records for an extended period of time. In accordance with Item 11b, records for projects that are implemented are to be destroyed five years after the project terminates. This proposed retention period will ensure that records germane to a requirement are available while the requirement is still current and for a period of time thereafter for use in developing new projects. In item 11c, installation and testing records are proposed for destruction or deletion 3 years after the final decision on acceptance is made. This retention period will ensure the

availability of records should problems develop and is also consistent with audit cycles.]

12. Electronic Mail and Word Processing System Copies

Electronic copies of records that are created on electronic mail and word processing systems and used solely to generate a recordkeeping copy of the records covered by the other items in this schedule. Also includes electronic copies of records created on electronic mail and word processing systems that are maintained for updating, revision, or dissemination.

a. Copies that have no further administrative value after the recordkeeping copy is made. Includes copies maintained by individuals in personal files, personal electronic mail directories, or other personal directories on hard disk or network drives, and copies on shared network drives that are used only to produce the recordkeeping copy. Destroy/delete within 180 days after the recordkeeping copy has been produced.

b. Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy. Destroy/delete when dissemination, revision, or updating is completed.

[*Appraisal analysis*: This item will provide disposal authority for electronic mail (email) and word processing records used solely to produce records described in GRS 24, after a recordkeeping copy has been produced, and electronic copies of records described in GRS 24 used solely for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy. In 1998 NARA added an item with the same wording as this item 12 to GRS 1–16, 18, and 23. Item 12 is in keeping with the authority that exists throughout the GRS to dispose of email and word processing copies of records within the scope of each GRS.

Agencies should use agency specific schedules developed following the guidance in NARA Bulletin 2001–03 or GRS 20 Items 13 and 14 to dispose of email and word processing copies of other information technology records (*i.e.*, records not covered by this GRS) that are not required for recordkeeping purposes. Please note that neither this item in GRS 24, the identical items in other GRS, nor GRS 20, items 13 and 14, apply to the copies of email and word processing records that are designated for recordkeeping purposes.]

Dated: May 16, 2002.

Michael J. Kurtz,

Assistant Archivist for Records Services—Washington DC.

[FR Doc. 02–16158 Filed 6–26–02; 8:45 am]

BILLING CODE 7515–01–P

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

Records Schedules; Availability and Request for Comments

AGENCY: National Archives and Records Administration (NARA).

ACTION: Notice of availability of proposed records schedules; request for comments.

SUMMARY: The National Archives and Records Administration (NARA) publishes notice at least once monthly of certain Federal agency requests for records disposition authority (records schedules). Once approved by NARA, records schedules provide mandatory instructions on what happens to records when no longer needed for current Government business. They authorize the preservation of records of continuing value in the National Archives of the United States and the destruction, after a specified period, of records lacking administrative, legal, research, or other value. Notice is published for records schedules in which agencies propose to destroy records not previously authorized for disposal or reduce the retention period of records already authorized for disposal. NARA invites public comments on such records schedules, as required by 44 U.S.C. 3303a(a).

DATES: Requests for copies must be received in writing on or before August 12, 2002. Once the appraisal of the records is completed, NARA will send a copy of the schedule. NARA staff usually prepare appraisal memorandums that contain additional information concerning the records covered by a proposed schedule. These, too, may be requested and will be provided once the appraisal is completed. Requesters will be given 30 days to submit comments.

ADDRESSES: To request a copy of any records schedule identified in this notice, write to the Life Cycle Management Division (NWML), National Archives and Records Administration (NARA), 8601 Adelphi Road, College Park, MD 20740–6001. Requests also may be transmitted by FAX to 301–837–3698 or by e-mail to *records.mgt@nara.gov*. Requesters must cite the control number, which appears in parentheses after the name of the agency which submitted the schedule, and must provide a mailing address. Those who desire appraisal reports should so indicate in their request.

FOR FURTHER INFORMATION CONTACT: Marie Allen, Director, Life Cycle Management Division (NWML), National Archives and Records Administration, 8601 Adelphi Road, College Park, MD 20740–6001. Telephone: (301) 837–3635. E-mail: *records.mgt@nara.gov*.

SUPPLEMENTARY INFORMATION: Each year Federal agencies create billions of records on paper, film, magnetic tape, and other media. To control this accumulation, agency records managers prepare schedules proposing retention periods for records and submit these schedules for NARA's approval, using the Standard Form (SF) 115, Request for Records Disposition Authority. These schedules provide for the timely transfer into the National Archives of historically valuable records and authorize the disposal of all other records after the agency no longer needs them to conduct its business. Some schedules are comprehensive and cover all the records of an agency or one of its major subdivisions. Most schedules, however, cover records of only one office or program or a few series of records. Many of these update previously approved schedules, and some include records proposed as permanent.

No Federal records are authorized for destruction without the approval of the Archivist of the United States. This approval is granted only after a thorough consideration of their administrative use by the agency of origin, the rights of the Government and of private persons directly affected by the Government's activities, and whether or not they have historical or other value.

Besides identifying the Federal agencies and any subdivisions requesting disposition authority, this public notice lists the organizational unit(s) accumulating the records or indicates agency-wide applicability in the case of schedules that cover records that may be accumulated throughout an agency. This notice provides the control number assigned to each schedule, the total number of schedule items, and the number of temporary items (the records proposed for destruction). It also includes a brief description of the temporary records. The records schedule itself contains a full description of the records at the file unit level as well as their disposition. If NARA staff has prepared an appraisal memorandum for the schedule, it too