BUREAU OF ENGRAVING AND PRINTING
CIRCULAR

No. 80-05.4

DATE December 18, 2006

POLICIES AND PROCEDURES FOR ELECTRONIC RECORDS AND EMAIL

1. PURPOSE AND SCOPE. This circular sets forth guidance regarding the creation, receipt, maintenance, use, and disposition of electronic records of the Bureau of Engraving and Printing (BEP/Bureau) to ensure compliance with policies established by the National Archives and Records Administration (NARA), the General Services Administration (GSA) and the Office of Management and Budget (OMB). It also provides information on scheduling the disposition of copies of program and administrative records created on electronic mail (email) systems, instant messaging (IM) applications, word processing systems, spreadsheets, and other automated information systems. Unless otherwise noted, these requirements apply to all BEP electronic records systems, whether on microcomputers, minicomputers, or mainframe computers, regardless of storage media, and regardless of whether in network or stand-alone configurations.

This circular also provides standards for the management of Federal records created or received on email and IM systems in the Bureau. Electronic source records of program and agency-specific administrative records created using these applications whose disposition is not covered by the General Records Schedule (GRS) that NARA issues, should be printed and filed in, or otherwise copied to, a recordkeeping system that is scheduled on a Standard Form 115, “Request for Records Disposition Authority,” approved by NARA. Only then may these records be deleted from the email or IM system.

This circular does not require the preservation of every email message. Its purpose is to ensure the preservation of those messages that contain information necessary for the adequate and proper documentation of BEP policies, programs, and activities. Email message creators and recipients must decide whether a particular message is appropriate for preservation. In making these decisions, all personnel should exercise the same judgment they use when determining whether to retain and file paper records. Email records, like all agency records, are subject to disclosure under the Freedom of Information Act and in litigation.

The provisions of this circular apply to all Bureau components.

2. REFERENCES.

a. “The Federal Records Act of 1950,” (44 United States Code (USC) Chapters 21, 29, 33 and 35), as amended;

b. “The Paperwork Reduction Act of 1995,” (Public Law 104-13), as amended;

c. "The Information Technology Management Reform Act (the Clinger-Cohen Act) of 1996," (Division E of Public Law 104-106);

d. "The Government Paperwork Elimination Act (GPEA) of 1998," (Public Law 105-277);

e. "The E-Government Act of 2002," (Public Law 107-347);

f. 36 Code of Federal Regulations (CFR) Chapter XII, Subchapter B, "Records Management";

g. "The Federal Management Regulation (FMR)," (41 CFR Parts 102-193, 102-194 and 102-195);

h. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources"; and

i. Treasury Directive 80-05 (TD 80-05), "Records and Information Management Program," dated June 26, 2002.

3. POLICY. It is the policy of the Bureau to:

a. ensure the effective and efficient management of electronic records throughout their life cycle from creation and receipt to final disposition;

b. preserve records needed for fiscal, legal, administrative, and historical purposes;

c. destroy in a timely manner information no longer needed for the conduct of current BEP business;

d. ensure cost effective use of automated data processing equipment, storage media, and other resources; and

e. ensure that electronically stored records can be retrieved and used when needed.

4. MANAGING ELECTRONIC RECORDS.

a. **Creation and Receipt of Electronic Records.** Any information that BEP creates or receives in carrying out its mission is a Federal record that must be stored and managed in accordance with applicable laws, regulations, and guidelines.

1) Electronic records are defined as those records stored in a form that only a computer can process, such as magnetic tapes, disks, drums, video files, and optical disk. Electronic records may include data files and data bases, machine-readable indexes, word processing files, electronic spreadsheets, electronic mail and messages and other text or numeric information, as well as internet/intranet sites. Electronic recordkeeping involves the use of a computer to create, retrieve, analyze, transmit, or delete electronic records.

2) The fact that information is created or stored electronically has no bearing upon whether that information is record or non-record. Record status is determined by the same criteria for all recorded information, regardless of the medium on which it is created or stored.

3) The decision about whether an electronic document is a record needs to be made earlier than for paper. Electronic records are more difficult to maintain because of the ease of erasing or changing the record, and the unique preservation requirements for electronic records.

4) Within BEP, there are two broad categories of electronic records:

(a) Records generated in a central automated data processing (ADP) facility that are created and used by data input personnel, computer operators, programmers, analysts, systems administrators, and/or remote users connected via local area networks (LAN).

i. Records in this category include files required to manage system housekeeping, performance tuning, system usage, log-in and password control, as well as audit trail files. Due to the administrative nature of these types of records, it is possible that they could be covered under the General Records Schedules (GRS). For more information about information technology (IT) records that might be covered under the GRS, contact the Documentation, Forms, and Records Management Division, Office of Enterprise Solutions.

ii. The majority of the records in this category is program-related and must be individually appraised for permanent or long-term value, particularly those databases created for action officers and/or offices that contain significant sets of statistical or analytical data not duplicated in paper records. Designers of systems that contain records in this category must ensure that adequate and up-to-date technical and security documentation for each system is maintained.

(b) Records created in an office setting.

i. Records in this category include word processing, spreadsheet, and database files; email 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 office.

ii. The record status of electronically stored drafts of policy documents should be re-evaluated as changes are made. Substantive updates to such electronic records probably constitute new records, while minor changes probably do not.

b. S**ecurity of Electronic Records**. Special precautions may need to be taken to ensure the security of data stored electronically. The need for any special security precautions should first be assessed by BEP IT managers. This can be done by following established risk-management techniques, keeping a reasonable ratio between the cost of the risk management study and the likely risk to be identified.

c. **Maintenance of Electronic Records.** In practice, there is no difference between maintaining electronic and paper records.

1) The contents of a computer's directory (e.g., everything on its “C:” drive) equates to the traditional file drawer. Each computer data sub-directory or electronic "folder" (e.g., everything in the “My Documents” folder) is the equivalent of a paper file folder. Files in sub-directories or "folders" (e.g., each word processing file in the My Documents folder) are individual "documents" in the folder. Sub-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 filed.

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

3) The management of electronic records is generally 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 BEP business should be deleted from the storage media in accordance with the appropriate record disposition schedules.

4) Information stored on disks/diskettes has a relatively short life expectancy estimated from one to five years. Consequently, any information on a disk that is required to be retained for longer periods should be converted to another medium to ensure its continued maintenance and readability. All diskettes should be labeled to specify their contents.

5) Office correspondence such as letters, memoranda, reports, and similar correspondence should always be printed out in hard copy form, so that a copy may be filed in the office files. In addition, the legend on this file copy should include an identification of the disk/diskette or hard drive on which the document is located. This will assist in retrieval of the disk/diskette or hard drive copy in case the document must be revised.

6) Other long-term records on disks/diskettes should be converted to magnetic tape, paper, CD-ROM, or microform. If conversion to magnetic tape is the best alternative, the conversion process and record sequence should be coordinated with the BEP Records Manager and NARA.

d. **Use of Electronic Records in Court Proceedings.**

1) It is possible for electronic records to be admitted in evidence in court proceedings (Federal Rule of Evidence 803[8]) if trustworthiness is established by thoroughly documenting the recordkeeping system's operation and the controls imposed upon it. BEP IT managers should implement the following procedures to enhance the legal admissibility of electronic records:

(a) Document that similar kinds of records generated and stored electronically are created by the same processes each time and have a standardized retrieval approach.

(b) Substantiate that security procedures prevent unauthorized addition, modification, or deletion of a record and ensure system protection against such problems as power interruptions.

(c) Identify the electronic media on which records are stored throughout their life cycle, the maximum time span that records remain on each storage medium, and the NARA-approved disposition of the records.

(d) Coordinate all of the above with the Office of the Chief Counsel and the Documentation, Forms and Records Management Program Division.

2) A strong records management program provides for information management and retrieval, complies with all applicable statutes, and addresses all applicable litigation matters, including court-ordered record retention requirements. The

Federal Records Act requires every Federal agency to develop and maintain an active, continuing records management program, and to have all agency records scheduled for disposition. This is accomplished through the General Records Schedule (GRS) that NARA issues and the BEP Comprehensive Records Schedule found at Exhibit A of the Records and Information Management Policies and Guidelines manual.

3) Record disposition schedules will be suspended for any records involved, or potentially involved, with litigation, claims, audit, or other actions. **It is the responsibility of the office having custody of such records to determine if such actions are pending before disposing of a record by contacting the Records Officer.** Employees must comply with all directives issued by the BEP to ensure that all documents and records, whether in paper, electronic, or other forms, are preserved if relevant to any aspect of litigation, investigation, or other actions.

e. **Inventorying of Electronic Records.**

1) Inventorying and scheduling the information within an automated information system are the most effective ways to ensure that BEP saves important data and deletes disposable data when no longer needed. Typically, the first step in the disposition process for electronic records is to prepare an inventory of what automated information systems exist, what they do and what they contain. BEP has already inventoried several automated information systems, either in response to requirements of oversight agencies, such as OMB and GSA, or as part of sound management of information resources.

2) If a comprehensive inventory of the information in an automated information system has been completed and is maintained, use that inventory to develop a records retention schedule for the electronic records in that system. If the inventory has not been completed, use the BEP Information System Description Form in Appendix A to develop and maintain a system inventory for that system. NARA uses the answers in the form to make an initial appraisal of the automated information system. BEP IT managers should use the inventory to develop a records retention schedule for the electronic records in that system.

f. **Retention of Electronic Records.**

1) How long any particular Federal record needs to be kept to facilitate the work of BEP, and the degree to which it needs to be controlled, is a function of its value to the mission or the agency, legal requirements, and its uniqueness.

2) Ensuring the retention of records electronically is not as simple as ensuring the retention of records stored on microform or paper. The ease with which

electronically stored records can be erased or changed increases the risk of unauthorized destruction, and alteration of official documentation and information.

3) Since electronic records are official records of the Federal government they may not be destroyed without proper authorization from NARA. BEP receives this authorization by scheduling the records using Standard Form 115, Request for Records Disposition Authority or using the GRS, if applicable.

4) If the same information is stored on more than one medium, such as paper and disk, BEP offices, in consultation with the BEP Records Officer and NARA must schedule each medium for disposition.

5) System managers must also pay close attention to all agency databases, including those that contain significant statistical data or information related to policy making functions, and schedule them for disposition.

6) The key to determining the appropriate retention period of any electronic or paper record 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. The factors include 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.

g. **Scheduling of Electronic Records.**

1) After identifying and inventorying existing automated information systems, the value of the information in each system must be determined. The first step in this evaluation process is for the system owner, in conjunction with system users, to decide how long BEP needs to keep the information (and in what form) for operational, legal, administrative, or fiscal purposes. The office of primary responsibility, system managers, and the users can best judge the usefulness of electronic records for current or future operations. NARA appraisers will review the recommendation and determine whether any of the records have enough potential value to warrant permanent preservation in the National Archives.

2) In developing any system that contains electronic records, the full life cycle of the records maintained in the system must be considered. System designers should contact the BEP Records Officer in the planning phase so that they can determine and incorporate records disposition requirements into the system design, development, and programming, thereby avoiding potentially costly changes after the system is established. Early involvement of the Records

Officer is especially critical in the case of major systems that may contain permanent records.

3) The development and implementation of records retention schedules requires coordination among several BEP officials: the Records Officer, information creators and users, and information systems managers, both functional and technical.

4) The first step in drafting a schedule for the disposition of temporary electronic records in a system is to determine whether those records are already covered by the GRS.

5) If the electronic records in a system are not covered by the GRS, separate disposition authority must be obtained to dispose of those electronic records. The disposition authority for all BEP-unique program electronic records (potentially permanent records) must be reviewed and approved by NARA. For all BEP electronic records that are not covered by an approved NARA disposition schedule, users should furnish the System Inventory Form to the BEP Records Officer. See Appendix A for an example of the form. The form is designed specifically for collection of the information needed to appraise the value of electronic records found in that system. Upon receipt of the form, the records management staff will consult the office having custody of the records and prepare a Standard Form 115, Request for Records Disposition Authority, and forward it to NARA for approval. The information required to complete the SF 115 is listed on the reverse side of the form. Appendix A also provides an example of a completed records schedule for an information system in a fictitious agency.

6) NARA appraises electronic records according to the same general standards it applies to any other records. Only one to three percent of Federal records have sufficient value to warrant permanent preservation in the National Archives. Permanent records document substantive program functions of an agency. Permanent records may also contain important and unique information about people, places, things, or events worthy of continued preservation for historical or research purposes.

7) NARA has reissued GRS 20, items 13 and 14, which apply to word processing and email copies. Items 13 and 14 authorize the disposal of electronic copies of scheduled records, **but only after a recordkeeping copy has been produced and filed in an acceptable recordkeeping system**. As a result of the re-issuing of GRS 20, items 13 and 14, NARA Bulletin No. 99-04, "Scheduling electronic copies of program records and administrative records not covered by the GRS," is suspended. BEP is required to schedule new and revised electronic records using Standard Form 115, Request for Records

Disposition Authority and submit it to NARA for approval. The SF 115 must include provisions for the disposition of both the copies of an electronic record that reside on email or other office automation applications, and the recordkeeping copy maintained in the recordkeeping system.

h. **Disposition of Electronic Records.**

1) Disposition means the actions taken regarding records when they are no longer needed for current government business and includes retirement to a Federal Records Center (FRC), transfer of permanent records to NARA, and destruction of temporary records.

2) All dispositions of Federal electronic records require the prior authorization of the Archivist of the United States. Federal electronic records may not be destroyed without the Archivist's approval of a disposition schedule.

3) Securing disposition authority for electronic records is often the same as scheduling information stored on any other medium such as paper or microfilm. Inventorying and scheduling are the most effective ways of ensuring that they are maintained only as long as needed.

4) All records are scheduled as either temporary or permanent. Temporary records are those the Archivist approves for disposal, either immediately or after a specified retention period. Permanent records are those the Archivist determines have sufficient value to warrant continued preservation by the government as part of the National Archives.

5) Record disposition schedules will be suspended for any records involved, or potentially involved, with litigation, claims, audit, or other actions. **It is the responsibility of the office having custody of such records to determine if such actions are pending before disposing of a record**. Employees must comply with all directives issued by the Bureau to ensure that all documents and records, whether in paper, electronic, or other form, are preserved if relevant to any aspect of litigation, investigation, or other actions.

6) If the routine disposition of records created by BEP employees and its contractors is suspended, the records officer or a representative from the Office of the Chief Counsel will notify the relevant offices. In situations involving a broad range or large magnitude of records subject to retention, the Director or his representative will issue and post notice of such action on the BEP Intranet site. Program managers have an obligation to inform contractors when disposition of relevant records is suspended. Program managers are also required to inform contractors when the suspension is lifted and routine disposition of the records

can recommence. If you have any questions on this process contact the Office of Chief Counsel.

7) Generally, electronic records are not forwarded to a FRC for retention pending disposal, because the FRC might not have specialized maintenance equipment to ensure the retention of data on magnetic tape for permanent files or for the long-term retention of temporary records. Temporary electronic records are not stored in the FRC. Therefore, custodial offices are responsible for the maintenance of the temporary records they create, whether in paper or electronic form, until the retention period has been met.

8) Electronic records scheduled for permanent retention are to be transferred annually to the National Archives at College Park or as soon as possible after their creation.

5. GUIDELINES FOR MANAGING ELECTRONIC MAIL.

a. **General Guidance.** All Federal employees (and Federal contractors) are required by law to preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency. Records must be properly stored and preserved, available for retrieval, and subject to appropriate approved disposition schedules.

1) The Federal Records Act applies to email records to the same extent as it applies to records that are created using other media. If you create or receive email messages during the course of your daily work, you are responsible for ensuring that you manage them properly.

2) The Department's current email policy requires that all emails and attachments that meet the definition of a Federal record be added to the organization's files by printing them (including the essential transmission data) and filing them with related paper records. If transmission and receipt data are not printed by the email system, annotate the paper copy. **In addition, if a notification from the Director, Chief Counsel, or their designated representative directs that litigation-related emails and attachments be forwarded or cc'd to a dedicated mailbox, employees must also send those emails to the prescribed mailbox.**

b. **Specific Questions and Answers.**

1) What is an email message?

An email message consists of any document created, transmitted, or received on an email system, including message text and any attachments.

2) When are emails records?

Emails are records when they:

- Are created or received in the transaction of agency business;
- Are appropriate for preservation as evidence of the government's functions and activities; or
- Are valuable because of the information they contain.

3) When are emails not records?

Emails are not records when they:

- Provide no evidence of agency functions and activities;
- Lack information of value; and
- Duplicate information already documented in existing records.

4) What are my responsibilities?

You are responsible for properly managing the creation, retention, and disposition of records that you send or receive on an email system. You must:

- Determine whether it is a record as soon as possible after you receive or send a message, including any attachments;
- Print a hard copy of the record, including attachments and transmission information, and file it in the official filing system**;**
- Delete the email version of the record unless you need it for reference purposes; and
- Delete messages and attachments that are not records as soon as they have served their purpose**.**

5) What about non-records...what do I do with them?

You should promptly delete non-record messages that are no longer needed unless they are the subject of pending litigation, a Congressional, Freedom of Information Act (FOIA), or internal retention directive. If non-record copies are useful for reference or convenience, you should copy the information to the hard drive of your computer or to a diskette. Examples of non-records include:

- Copies of memorandums or text sent for information rather than action;

- Instruction memorandum or information bulletins, where the recipient is not the action office; and
- Messages that have only temporary value such as a message that a meeting time has changed.

Warning: Do not delete a message or attachment that is the subject of a Congressional, FOIA, or discovery request or that is needed for litigation even if it may constitute a non-record (unless it has been previously printed and, if applicable, copied or forwarded to a dedicated mailbox established by BEP to store such emails and attachments).

6) If I file my email message in a folder created in my email system, do I still have to print it and file it in the office filing system?

Yes. Email folders are part of the email system and cannot be part of an official filing system because the email system is protected by use of an individual password accessible only to you. Remember, records must be available for retrieval and access by those who need them.

7) What about copies of documents on my laptop computer...are they records?

All documents (email, word processing, spreadsheets, etc.) on a laptop that meet the definition of a record (See Item #4-A.1-Creation and Receipt of Electronic Records) are considered to be separate documents from similar documents maintained on the computer in your office until they are synchronized and identical.

8) Can I use email on my government computer to send personal messages?

The Bureau permits employees who are granted email access for official purposes, to make limited personal use of such access during non-work time for reasonable duration and frequency of use. Email access is a privilege, not a right, and employees must be familiar with the policies and procedures that apply to such use, including the BEP Employee Handbook and BEP Manual No. 10-08.35, Chapter 2-2-1, "Electronic Mail." Unauthorized or improper use of email may result in disciplinary and/or corrective action, suspension of email privileges, financial liability for the costs associated with misuse, and/or criminal prosecution. Personal email messages do not promote the Bureau's mission, therefore, are not Federal records and should not be stored.

Employees are also reminded that any email, official or personal, sent, received, or accessed using BEP equipment or IT resources is subject to monitoring, recording, and disclosure to authorized officials. Employees should have no expectation of privacy with regard to such communications.

9) What about Instant Messaging (IM) applications…are the messages they create considered Federal Records?

Yes, as with email messages, instant messages can be Federal records when they are created or received in the transaction of agency business, are appropriate for preservation as evidence of the government's functions and activities, or are valuable because of the information they contain. A common misconception about instant messages is that there is no record of the exchange on the computer's hard drive. An instant message may be recovered from a computer depending on factors such as the type of IM software used, software configuration, type of computer operating system, and the date of the message. If the instant message can be considered a Federal record, then the user should print out the IM conversation and file it in the appropriate BEP recordkeeping system.

10) We were recently issued Blackberry Wireless Handhelds in our office. What are the records management implications for these devices?

You can use these devices to send and receive email. These emails can be Federal records when they are created or received in the transaction of agency business, are appropriate for preservation as evidence of the government's functions and activities, or are valuable because of the information they contain. Make sure that your Blackberry is copying all of your emails to your desktop computer when you connect it to its desktop cradle at the end of the day. These emails could be Federal records and should be managed appropriately in accordance with the BEP electronic mail guidance. Please contact the Help Desk immediately if your Blackberry is not backing up your emails to your desktop when connected to the cradle.

11) What about Voice Mail?

Generally, a voice mail system is not considered to be a recordkeeping system. Voice mail messages are automatically deleted from the voice mail after a short time (currently, 30 days). If the content of a voice mail message is appropriate to preserve as a record, then the user needs to take measures to document the message in an appropriate BEP recordkeeping system. For example, the content of the voice mail message can be recorded on paper, or in an electronic file, either as a "note to file" or in a confirming note or memorandum to the sender of the voice mail message, and then be filed in a

recordkeeping system. If the content of a voice mail message is determined to be a record, the audio version of the message may be deleted once the content has been properly documented in a regular recordkeeping system. The audio version of a message should not be deleted, and affirmative steps should be taken to preserve it in audio form outside the voicemail system, if the audio version itself would be useful in investigating or documenting a claim, a threat, improper conduct, etc., or if the audio version is required to be retained pursuant to an internal retention directive. **For specific instructions on preserving the audio version of voice mails, contact the BEP Help Desk.**

12) Is there anything else I need to know?

Yes, quite frequently, emails are involved in a discovery process during litigation, and/or the subject of congressional requests and FOIA requests. If you have emails that are involved in active cases, those emails must be preserved by printing them, and, if so directed in a notification from the Director, Chief Counsel, or their designated representative, by also sending them to a dedicated mailbox. Specific requirements regarding the preservation of relevant FOIA documents are provided by the Office of Chief Counsel or the BEP Disclosure Officer.

For BEP records management questions, contact BEP's Documentation, Forms and Records Management Division.

6. RESPONSIBILITIES.

a. RESPONSIBILITY FOR ISSUANCE OF GUIDANCE.

NARA issues standards for the management of Federal records created or received on electronic systems. These standards apply to all Federal agency offices using office automation or information systems and will be followed by the Bureau. The complete version of 36 CFR Part 1234-"Electronic Records Management," is available online at http://www.archives.gov/about_us/regulations/part_1234.html

The authority delegated to the Director, Bureau of Engraving and Printing, by Treasury Directive 80-05 (TD 80-05), dated June 26, 2002, is hereby designated to the Manager, Documentation, Forms and Records Management Division, to be exercised with respect to the Records Management Program.

b. **PROGRAM MANAGEMENT.**

1) The Manager, Documentation, Forms and Records Management Program Division, serves as the BEP Records Officer and has oversight responsibility for the development, direction, and implementation of the BEP Records Management Program. The BEP Records Officer shall:

(a) Integrate the management of electronic records with other records management programs of BEP;

(b) Incorporate electronic records management objectives, responsibilities, and authorities in pertinent BEP directives and disseminate them throughout BEP as appropriate;

(c) Establish procedures for addressing electronic records management requirements, including disposition, before BEP approves new electronic records systems or enhancements to existing systems;

(d) Ensure that systems owners develop and maintain up-to-date technical documentation for each electronic records system that produces, uses or stores data files;

(e) Develop and secure NARA's approval of records disposition schedules for electronic systems that produce, use, or store data files;

(f) Ensure that BEP develops and maintains up-to-date comprehensive system inventories to include all major and administrative systems (including websites) using the BEP Information System Inventory or a comparable form and ensure that the systems are included in the Department's Government Information Locator Service (GILS);

(g) Ensure compliance with applicable Government-wide policies, procedures, and standards, such as those issued by OMB, the Government Accountability Office (GAO), NARA, and the National Institute of Standards and Technology (NIST);

(h) Review electronic records systems periodically for conformance to established BEP procedures, standards, policies, and directives as part of the periodic reviews required by 44 USC 3506;

(i) Ensure that electronic records systems that maintain the official file copy of text documents on electronic mail meet the following requirements:

i. Provide a method for authorized users of the systems to retrieve the desired documents, such as an indexing or text search system;

ii. Provide an appropriate level of security to ensure integrity of the documents;

iii. Provide a standard interchange format, when necessary, to permit the exchange of documents on electronic media between the Department's computers using different software/operating systems and the conversion or migration of documents on electronic media from one system to another; and

iv. Provide for the disposition of documents including, when necessary, the requirements for transferring permanent records to NARA;

(j) Ensure that before a document is created electronically on electronic recordkeeping systems that will maintain the official file copy on electronic media, each document shall be identified sufficiently to enable authorized personnel to retrieve, protect, and carry out the disposition in the system;

(k) Ensure that BEP selects appropriate media and systems for storing electronic records throughout their lifecycle;

(l) Ensure that electronic records scheduled for destruction are disposed of in a manner that protects any sensitive, proprietary, or national security information;

(m) Ensure that BEP instructions on identifying and preserving email messages address the following unique aspects of email messages:

i. Some transmission data (names of sender and addressee(s) and date the message was sent) must be preserved for each email record in order for the context of the message to be understood. BEP shall determine if any other transmission data are needed for purposes of the context.

ii. Offices that use email systems that identify users by code or nicknames or identify addresses only by the name of a distribution list shall instruct staff on how to retain names on directories or distribution lists to ensure identification of the sender and addressee(s) of messages that are records.

iii. Offices that use an email system that allows users to request acknowledgements or receipts showing that a message reached the mailbox or inbox of each addressee, or that an addressee opened the

message, shall issue instructions to email users specifying when to request such receipts or acknowledgements for recordkeeping purposes and how to preserve them.

iv. Offices with access to external email systems shall ensure that Federal records sent or received on these systems are preserved by printing and filing the Federal records in the appropriate recordkeeping system and that reasonable steps are taken to capture available transmission and receipt data needed for recordkeeping purposes.

v. Those email systems that provide calendars and task lists, which meet the definition of Federal records, are to be managed in accordance with the provisions of GRS 23, Item 5.

vi. Draft documents that are circulated on email systems may be records if they meet the criteria specified in 36 CFR 1222.34;

(n) Consider the following criteria when developing procedures for the maintenance of email records in appropriate recordkeeping systems, regardless of format.

Recordkeeping systems that include email messages must:

i. Provide for the grouping of related records into classification according to the nature of the business purposes the records serve;

ii. Permit easy and timely retrieval of both individual records and files or other groupings of related records;

iii. Retain the records in a usable format for their required retention period as specified by a NARA-approved records schedule;

iv. Be accessible to individuals who have a business need for information in the system;

v. Preserve the transmission and receipt data specified in bureau instructions; and

vi. Permit transfer of permanent records to NARA;

(o) Ensure that BEP will not store the recordkeeping copy of email messages that are Federal records only on the email system, unless the system has all of the features specified above in paragraph (n) of this section. If the email

system is not designed to be a recordkeeping system, BEP shall print and file the Federal records to a recordkeeping system.

2) The CIO, in collaboration with the Chief of Critical Infrastructure and IT Security and the Chief of IT Operations, shall:

(a) Establish and implement policies and procedures to guard against the unauthorized destruction, loss, removal, or theft of electronic records;

(b) Exercise responsibility for the overall administration of the automated information systems (AIS) security program, which includes measures to protect electronic recordkeeping systems;

(c) Ensure that adequate training is provided for users of electronic records systems in the operation, care, and handling of equipment;

(d) In collaboration with BEP Program managers, specify the location, manner, and media in which electronic records will be maintained to meet all operational and archival requirements, and maintain inventories of electronic records systems to facilitate disposition;

(e) Specify the methods for implementing controls over national security-classified, sensitive, proprietary, and Privacy Act records stored and used electronically;

(f) Implement and maintain an effective records security program that incorporates the following:

i. Ensures that only authorized personnel have access to electronic records;

ii. Provides for backup and recovery of records to protect against information loss;

iii. Ensures that appropriate agency personnel are trained to safeguard sensitive or classified electronic records;

iv. Minimizes the risk of unauthorized alteration or erasure of electronic records; and

v. Ensures that electronic records security is included in computer systems security plans prepared pursuant to the Computer Security Act of 1987 (Public Law 100-235, 44 U.S.C. 3505 note).

(g) Ensure that magnetic recording media previously used for electronic records containing sensitive, proprietary, or national security information are not reused if the previously recorded information can be compromised by reuse in any way.

3) The Associate Directors, in concert with the BEP Records Officer, are responsible for the execution of the electronic records management program in their respective areas. They shall:

(a) Designate a qualified Records Liaison Officer for each office and an alternate for the execution of the programs in each Directorate.

(b) Assign to the Records Liaison Officer the responsibility for carrying out the following program functions:

i. Maintain close liaison with the BEP Records Officer and assist with the implementation of the records management program in their Directorates to assure adherence to provisions of all BEP directives pertaining to the program;

ii. Provide adequate controls over the creation and location of file stations and contact the BEP Records Officer to initiate actions necessary for the transfer of records between activities within BEP or to another agency; and

iii. Review and evaluate existing or new records series and electronic systems to develop disposition schedules, and prepare and submit proposed disposition schedules to the BEP Records Officer for review and approval.

4) BEP Program Managers (system owners) shall oversee the creation and use of records in an information system. Program managers who currently operate an electronic system of records or plan to develop a new system of records are responsible for ensuring that the requirements of this section are implemented for their systems. They are responsible for managing those systems under their functional control and for maintaining those systems in accordance with electronic recordkeeping guidelines. Respective program managers will coordinate electronic records system activity with the BEP Records Officer in order to:

(a) Identify the official source of record for the records being created;

(b) Determine if the data are Federal records or not;

(c) Determine in what form the official record will be maintained for its lifecycle (i.e., paper, microform, tape, disk, diskette, or CD-ROM);

(d) Establish procedures for identifying, cataloging, and labeling records when they are created;

(e) Provide and verify system description information on the BEP Information System Inventory (or comparable form) to the appropriate office to develop the BEP information system inventory;

(f) Follow the applicable records management guidance in TD P 84-01, (Information System Life Cycle Manual) when developing information systems; and

(g) Ensure that adequate system documentation is created and maintained for the life of the records to which it relates.

5) Information creators and/or content providers, including contractors doing business with BEP, and automated system and word processor users are responsible for:

(a) Ensuring that all machine-readable and electronic records are properly maintained and disposed of in accordance with the provisions of this section, Exhibit A, BEP Circular No. 80-05, "Records Management Program," BEP's Record Schedule, NARA's GRS, and all BEP record retention directives;

(b) Notifying the BEP Records Officer when planning a new system or new applications;

(c) Determining what records each individual or group is responsible for creating and maintaining;

(d) Becoming familiar with the requirements of this section;

(e) Identifying and describing the applications supported by automated systems by means of defining their purposes, their information contents, and the main stages through which the data flow;

(f) Determining the length of time the information is needed to support organization operations and protect legal and financial rights;

(g) Describing the indexing arrangement and, to the extent possible, the internal information structure and search possibilities; and

(h) Documenting and implementing disposition instructions on an approved records schedule.

7. OFFICE OF PRIMARY RESPONSIBILITY. Office of Enterprise Solutions.

<SIGNED>
Peter O. Johnson
Associate Director (Chief Information Officer)

Distribution - Office Chiefs – DCF
Division Managers - WCF

APPENDIX A: BEP INFORMATION SYSTEM DESCRIPTION FORM

Electronic records are most effectively and conveniently inventoried and scheduled in the context of information systems. An information system is the organized collection, processing, transmission, and dissemination of information according to defined procedures. It includes four categories of information: (1) inputs, (2) the information on the electronic media, (3) outputs, and (4) documentation.

Elements of the Information System Inventory

Each Office should maintain a complete and accurate inventory of all its electronic record systems to meet its own needs and to comply with the National Archives and Records Administration (NARA) regulations (36 CFR 1234). Consultation with Information Technology (IT) personnel may be necessary in order to answer some of these questions. This inventory should include the elements indicated below.

1. System title.
2. System control number.
3. Name of agency program supported by system.
4. Program authority.
5. System description, including:
   a). Purpose/function of system;
   b). Sources of data (include inputs from other systems);
   c). Information content (include examples of data fields);
   d). System outputs (include outputs to other systems);
   e). Documentation (manuals, record layouts, data dictionaries, etc);
   f). Recommended disposition for inputs;
   g). Recommended disposition for electronic data;
   h). Recommended disposition for outputs;
   i). Recommended disposition for documentation; and
   j). Hardware/software environment.
6. Privacy Act System Notice and associated Federal Register documentation, if applicable.
7. Indicate whether or not there are any restrictions on the release to the public of the data.
8. Indicate whether or not the records are vital records.
9. Indicate whether or not the records are subject to litigation in which BEP is involved. If so, cite case(s).
10. Superseded NARA job citation number(s), if applicable.
11. Agency contacts (names, addresses, and phone numbers of system and program personnel) that can provide additional information about the system and the program it supports.
12. Preparer's name, signature, and date.
13. Office name and address (building, room number, and telephone number).

BEP INFORMATION SYSTEM DESCRIPTION FORM	
1. System Title	2. System Control Number
3. Agency Program Supported by System	4. Program Authority
5. System Description	
a. Purpose/Function of System	
b. Sources of Data (Include inputs from other systems)	
c. Information Content (Include examples of data fields)	
d. System Outputs (Include Outputs to Other Systems)	

e. Documentation (Manuals, record layouts, data dictionaries, etc.)

f. Recommended disposition for inputs

g. Recommended disposition for electronic data

h. Recommended disposition for outputs

i. Recommended disposition for documentation

j. Hardware/software environment

6. a) Are the records in this system subject to the Privacy Act? Yes ☐ No ☐

b) Is there a published notice of routine use that applies to the records? Yes ☐ No ☐

If Yes, cite the agency system number and Federal Register volume and page number of the most recent notice and attach a copy of the most recent notice.

7. Are there any restrictions on the release of the data to the public?

Yes ☐ No ☐

If Yes, please cite the authority for those restrictions:

8. Are the records in the system necessary to protect the legal and financial rights of the government or individuals affected by the government (vital records)?

Yes ☐ No ☐

9. Are the records subject to litigation in which FMS is involved? If so, please cite the case(s). Yes ☐ No ☐

10. Superseded NARA job citation number(s) if applicable

11. Agency contacts (names, addresses, and phone numbers of system and program personnel who can provide additional information about the system and the program it supports: _____ _____ _____	
12. Preparer's Name, Signature, and Date	13. Office Name and Address (Building, Room Number, and Telephone Number)

Explanations

1. The commonly used name and acronym of the system (e.g., Budget System, Grain Monitoring System (GMS), etc.)

2. The internal control number assigned to the system for reference, control, or cataloging purposes (e.g., Information System Inventory Number, ADP Plan control number, etc.)

3. What agency programs or mission does the system support?

4. What laws, directives, etc., authorize these programs or mission?

5. System Description has the following sections:

   a) *Purpose/Function*: The reasons for and the requirements met by the system.

   b) *Sources of Data*: The primary sources or providers of data to the system (e.g., certified requests for payment disbursements from Federal agencies, corporations doing business in the US, etc.). Does this system receive information from other systems, either from within or outside BEP? If yes, please indicate systems.

   c) *Information content*: The principal subject matter, data coverage, time span, geographic coverage, update cycle, whether the system saves superseded information, examples of data fields, and major characteristics of the system.

   d) *Outputs*: The principal products of the system (e.g., reports, tables, charts, graphic displays, catalogs, correspondence, etc., and an indication of the

frequency of preparation). Is information from this system transferred to other systems? If yes, please indicate information transferred and name of system that receives this information.

e) *Documentation:* Information about the system. Documentation might be in electronic or hardcopy media and might be found in publications, administrative reports, annual reports, memorandums, user notes, system guides, Privacy Act notices, or manual or automated data dictionaries.

f-i) *Recommended Disposition*: How long does BEP need the records for administrative, legal, or fiscal purposes, that is, to document its conduct of the public business? Has NARA previously approved a records schedule for these records? If yes, please indicate the NARA job citation, e.g., N1-318-00-1, and the item number in the job applicable to these records in item 9 of this form.

j) *Hardware/software environment*: Indicate the computer system manipulating this information and the software used.

6. *Privacy Act System of Records*: The Privacy Act notice applies only to a set of records (in any format) from which information is retrieved by the individual's name or other personal identifiers. If applicable, please cite the agency system number and Federal Register volume and page number of the most recent Privacy Act notice and attach a copy of the most recent notice. Seek guidance from the BEP Disclosure Officer if needed.

7. Are the records fully available for public use? If the records are exempt from release pursuant to the FOIA, 5 USC 552(b)(1)-(9) and (c)(1)-(3), this must be fully justified. List all exemptions that apply.

8. *Vital Records*: Essential agency records that are needed to meet operational responsibilities under national security emergencies or other emergency or disaster conditions (emergency operating records) or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records).

9-13. Self-explanatory.

Example of a Completed Database Schedule

Agency: Office of Economic Concerns (OEC)*

Name of system: Grant Profile Information System (GPIS)
Unit: Office of Grant Operations provides executive direction and guidance to regional OEC offices responsible for compiling grant profile information under Section 402 (c) (11) of the Grants in Government Act.

Purpose of System: Supports OEC regional offices function of complying with legal requirements for awarding federal grants. System compiles financial and organizational information about each grant recipient.

1. **Inputs:** Electronic and paper (SF 123) inputs consisting of budget data, organizational profiles, including principal offices, board compositions, and private/non-profit status.

Disposition: Temporary. Delete or destroy after input and verification of data into master file or when no longer needed to support the reconstruction of the master file, whichever is later.

2. **Master file:** Budget data, organizational profiles, and data on public and private involvement in the project. The system contains records created from 1995 to the present. One database record is created for each grant recipient. The primary key is the grant number.

Disposition: Temporary. Delete record 6 years after close out or termination of grant.

3. **Outputs:** Grant profile summary reports (supersedes N1-575-98-1, item 15).

a. Electronic copy:

Disposition: Temporary. Delete after recordkeeping copy is produced or when no longer needed for operational purposes, whichever is later.

b. Recordkeeping copy (paper).

Disposition: Temporary. Cut off at end of calendar year. Retire to records storage facility 2 years after cutoff. Destroy 6 years after cutoff.

4. **System Documentation.**

a. Codebooks, record layout, and other system documentation.

Disposition: Temporary. Cut off when system is replaced. Transfer to records storage facility 1 year after cutoff. Destroy 6 years after cutoff.

b. Word processing and email copies of records covered by item 4a. of this schedule.

Disposition: Temporary. Delete when recordkeeping copy is produced.

*[This is a fictitious agency.]

APPENDIX B: GLOSSARY OF TERMS

1. Adequate and proper documentation. This term means a record of the conduct of Government business that is complete and accurate to the extent required to document the organization, functions, policies, decisions, procedures, and essential transactions of the agency and that is designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities.

2. Authenticity. A condition that proves a record is authentic and/or genuine based on its mode, form, state of transmission, and manner of preservation and custody.

3. Computer output microform (COM). Microfilm containing data produced by a recorder from computer-generated signals.

4. Destruction. The destruction of records includes physically destroying the record material itself, or removal of the informational content. Records authorized for destruction will be:

   a) Destroyed by pulping, burning, or macerating if this action is necessary to avoid disclosure of information that might be prejudicial to BEP, public, or private interests. Documents containing social security numbers and applicable names must be shredded or burned; and

   b) Erased and reused, if appropriate, when the records are on machine readable and/or electronic media.

5. Disposition. This term means the retirement, transfer, donation, or destruction of records.

6. Disposition authority. Approval of the National Archives and Records Administration (NARA) reflected on a SF-115, empowering an agency to transfer permanent records to the National Archives or carry out the disposal of temporary records. **This disposition authority may be suspended by court orders or internal agency directives**.

7. Documentation. Systems information needed to read and understand the data. Documentation might be in publications, administrative reports, annual reports, memoranda, user notes, system guides, Privacy Act notices, or manual or automated data dictionaries.

8. Electronic record. This means any information that is recorded in a form that only a computer can process and that satisfies the definition of a Federal record in 44 USC 3301.

9. Electronic information system. A system that contains and provides access to computerized Federal records and other information.

10. Electronic mail system. A computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities (software that transmits files between users but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or data bases on either personal computers or mainframe computers, and word processing documents not transmitted on an email system.

11. Electronic recordkeeping system. An electronic system in which the official file copies of electronic records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition.

12. Emergency-operating records. That type of vital records essential to the continued functioning or reconstitution of an organization during and after an emergency. Included are emergency plans and directives(s), orders of succession, delegations of authority, staffing assignments, selected program records needed to continue the most critical agency operations, as well as related policy and procedural records that assist agency staff in conducting operations under emergency conditions and for resuming normal operations after an emergency.

13. General Records Schedules (GRS). NARA-issued schedules governing the disposition of specified temporary records common to several or all agencies. They give Federal agencies the authority to dispose of such records without further approval from NARA.

14. Legal and financial rights records. These records are the type of vital records essential to protect the legal and financial rights of the Government and individuals directly affected by its activities. Examples include accounts receivable records, social security records, payroll records, retirement records, and insurance records. These records were formerly defined as "rights-and-interests" records. Records that have the properties of both emergency-operating and legal and financial rights records are treated as emergency-operating records.

15. Life cycle of records. The management concept that records pass through three stages: creation (and receipt), maintenance and use, and disposition.

16. Non-record materials. Materials, as defined in 36 CFR 1220.14, such as extra copies of documents, kept solely for reference, stocks of publications and processed documents, and library or museum material intended solely for reference or exhibits.

17. Permanent record. This term applies to any Federal record that has been determined by NARA to have sufficient value to warrant its preservation in the National Archives.

18. Preservation. The basic responsibility to provide adequate facilities for the protection, care, and maintenance of records.

19. Recordkeeping system. This is a manual or automated system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition.

20. Records. The Records Disposal Act of 1943, as amended (44 USC 3301), defines "records" as: "...all books, papers, maps, photographs, machine-readable, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the informational value of the data in them."

21. Records maintenance and use. This term means any activity involving the location of records of a Federal agency or the storage, retrieval, and handling of records kept at office file locations by or for a Federal agency.

22. Records management. This term means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation and receipt, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective economical management of agency operations.

23. Records schedule. A document providing the legal authority to dispose of records. Schedules contain the records description and disposition instructions approved by NARA.

24. Temporary records. A temporary record is any record which has been determined by the Archivist of the United States to be disposable in: (1) an agency schedule; (2) a General Records Schedule (GRS); or (3) an approved one-time authorization to dispose of the records.

25. Transfer. Disposition includes the transfer or a change of custody from one organization or agency to another. Records may be transferred to another office as a result of the realignment of functions or reorganization without prior approval from the Archivist of the United States. However, any other transfer of records to another office or agency must be approved by the Archivist of the United States.

26. Transmission and receipt data.

a) Transmission data. Information in electronic mail systems regarding the identities of sender and addressee(s), and the date and time messages were sent.

b) Receipt data. Information in electronic mail systems regarding date and time of receipt of a message, and/or acknowledgment of receipt or access by addressee(s).

27. Unscheduled records. These are records whose final disposition has not been approved by NARA. Unscheduled records are those not disposable under the General Records Schedules (GRS); those that have not been included on a Standard Form (SF) 115, "Request for Records Disposition," approved by NARA; those described but not authorized for disposal on an SF 115 approved prior to May 14, 1973; and those described on an SF 115 but not approved by NARA (withdrawn, canceled, or disapproved).

28. Vital Records. These are essential agency records that are needed to meet operational responsibilities under national security emergencies or other emergency or disaster conditions (emergency operating records) or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records).