INFORMATION GOVERNANCE AND LIFECYCLE MANAGEMENT MANUAL

CHAPTER 230
MANAGING UNSTRUCTURED DATA AS INFORMATION ASSETS

TABLE OF CONTENTS

230.01 PURPOSE

This chapter provides information governance policies and guidance for Unstructured Data Management (UDM) to comply with National Archives and Records Administration (NARA) regulations on lifecycle management of Federal record material in electronic format and use of a BPA Electronic Recordkeeping System (ERKS) under those regulations.

230.02 BACKGROUND/OVERVIEW

A. BPA uses a variety of unstructured data formats to create, receive, manage and maintain its information assets. These include the Microsoft Office suite of applications, email and digital image formats. The nature of unstructured data allows great flexibility in supporting business processes and creating work product, but that same flexibility can present challenges for the agency to appropriately manage, maintain and dispose of information assets in unstructured data formats:

- Information in unstructured data formats may not be uniform: the content may concern any subject or function.
- The content (and therefore its business value) may not be immediately discernible from the file name.
- Important metadata for understanding the context in which the information asset was created or received may not be easily accessible or could be missing.

- Without recordkeeping capabilities, easy and timely retrieval of information contained in unstructured data formats (whether individually or in sets of related information assets) may be difficult.
- Ensuring that record material is timely and appropriately disposed according to its scheduled retention period as required by the Agency File Plan is not an inherent part of unstructured data format applicaitons.
- Unstructured data formats used to maintain long-term records (e.g., ten-year retention or more) may become obsolete, such that the content contained in those formats is effectively lost.

B. Meeting BPA's regulatory obligations for managing its information assets, as well as facilitating BPA's producing information as required through litigation or other requests, requires that policies, procedures and technology standards are implemented that will appropriately address these special challenges.

230.03 TERMINOLOGY

See Chapter 003 for all terms and definitions associated with IGLM. As used in this Chapter, the following acronyms and definitions apply:

230.03.1 Acronyms

EIS	Electronic Information System
ERKS	Electronic Recordkeeping System
IGLM	Information Governance and Lifecycle Management
NARA	National Archives and Records Administration
OGC	Office of General Counsel
SEIS	Structured Electronic Information System
UDM	Unstructured Data Management

230.03.2 Definitions

CLASSIFICATION	Identifying and applying metdata to an information asset that includes 1) the business function; 2) a date/timestamp 3) the retention period; 4) the office of record; and 5) the author or custodian of the record according to the taxonomy approved by the Agency Records Officer.
ELECTRONIC INFORMATION	Recorded information in electronic format (requiring computer technology to retrieve or access); digital content. This definition includes both the content of the information asset and associated metadata.
ELECTRONIC INFORMATION SYSTEM (EIS)	Computerized/digital means for collecting, organizing, and categorizing information to facilitate its preservation, retrieval, use, and disposition. These systems contain and provide access to Federal records and other information.
ELECTRONIC RECORDKEEPING SYSTEM (ERKS)	See Structured Electronic Information System (SEIS); any SEIS that is substantially compliant with either the DoD 5015.2 or the F1000 standards for integrity, security, and disposition.

FEDERAL RECORD	Recorded information in any medium 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 data in them. Materials made or acquired solely for reference, extra copies of documents preserved only for convenience of reference and stocks of publications are not included. - *see* Federal Records Act, 44 USC §3301.
METADATA	Structured information about any recorded information such as date and time the recorded information was created, author, organization or other data. This also includes descriptions of content, structure, data elements, interrelationships, and other characteristics of data, information and records as well as information asset profiles or indexing data.
OFFICE OF RECORD	The organization that, by definition of its mission or function, has primary responsibility for maintenance and retention of the record.
SHORT-TERM RECORD	Recorded information that may provide some evidence of the agency's organization, functions or activities, but is in an incomplete or draft form. Short-term records have a retention period of no more than two years.
STRUCTURED ELECTRONIC INFORMATION SYSTEM (SEIS)	Electronic information systems (EIS) used by BPA to collect/maintain data or records in a structured format (typically a database). These systems are required to have a complete, approved Structured Electronic Information System Schedule form (1324.02e) submitted to the IGLM team as part of the System Lifecycle (SLC) process. Electronic Recordkeeping Systems (ERKS) are a sub-set of SEIS that meet additional records compliance requirements.
TRANSITORY RECORDED INFORMATION	Recorded information with no continuing business value. This may also include recorded information made or acquired solely for reference, extra copies of documents preserved only for convenience and stocks of publications. Transitory recorded information has a retention period of no more than ninety days.
UNSTRUCTURED DATA MANAGEMENT (UDM)	Policies, services and tools that aid in appropriately managing electronic information that is not contained in a database or SEIS. UDM is designed to manage unstructured data throughout the information lifecycle.

IGLM Manual
Chapter 230
Managing Unstructured Data as Information Assets

230.04 APPLICABILITY/SCOPE

A. Consistent with BPA Manual chapter 1110 and IGLM chapter 12, this chapter applies to all personnel (users) who create, receive or access information assets in electronic information systems (EIS), regardless of the information asset's form or format. The form or format includes but is not limited to the Microsoft Office Suite of products (e.g., Word, Excel, etc.), email (including pst files), and digital image formats (e.g., pdf, gif, tiff, etc.).

B. This policy applies to all information assets created, managed or maintained in the UDM environment. The UDM environment includes the myPC server environment as well as the EIS identified in IGLM chapter 12, section 05.3 - 8. Other guidance applicable to a specific medium may apply (e.g., IGLM chapter 260 – Email Systems – User Policies and Guidance). The policy is applicable to any technology solutions developed to create or manage an integrated agency UDM environment, whether as an archiving solution or an indexing solution applied to existing information asset locations (e.g., SharePoint, shared drives, etc.).

C. In addition to the information governance policies of this chapter, all users are responsible for adhering to BPA's policies on Business Use of Information Technology Services (see BPA Manual chapter 1110.F) and Cyber Security requirements.

230.05 POLICY INFORMATION

A. As stated in IGLM chapter 11, BPA's IGLM policies are media-neutral. Information assets within the UDM environment must be managed according to their content, not their format. The objectives of unstructured data management are to:

1. Maintain consistent, enforced retention policies;
2. Enable faster access;
3. Effectively organize emails and information;
4. Improve efficiency; and
5. Reduce physical storage.

B. Users creating or receiving information assets in unstructured data format shall organize, manage, maintain and dispose of them in a consistent fashion throughout BPA. This may be accomplished through functionality that is built into electronic information systems (i.e., an archiving/ indexing application); by transferring information assets to an electronic recordkeeping system (ERKS) such as an archive; or some combination of both; collectively these alternatives are referred to as "UDM systems." The policies in this chapter are designed to accommodate UDM systems or other technology solutions for efficiency and effectiveness as well as ensuring internal controls for compliance with laws and regulations applicable to government information assets.

IGLM Manual
Chapter 230
Managing Unstructured Data as Information Assets

230.05.1 Short-Term Records, Transitory Recorded Information

A. Users may manage and maintain Information assets meeting the definition of either transitory recorded information or short-term records in any EIS (including SharePoint sites or networked drives) for their respective retention periods (90 days and two years).

B. Transitory Recorded Information. Because of the lack of business value in transitory recorded information, users should delete such material as quickly as possible but in any case, within ninety days of creation or receipt. Generally, such material should not be stored in the same EIS or locations as short-term records and must not be managed or maintained with Federal records. Because the UDM environment does not have an auto-delete function, all users must actively manage any transitory recorded information they create or receive to ensure it is deleted in a timely manner.

C. Short-Term Records. Short-term records require basic metadata for organizing purposes including a creation date, a last accessed/modified date and an office of record. Usually, the office of record may be identified by the SharePoint site or network drive folder in which the information asset is maintained. Only convenience copies of short-term record material should be maintained on a hard drive, personal network drive, thumb drive or flash drive (also know as a USB). If circumstances require a short-term record being maintained in one of these locations, the record must be moved to an office of record SharePoint site or network drive as soon as practical. Short-term records require a consistent file naming convention or application of a series of metadata to assist users in easily locating and identifying the record. Each office of record is responsible for developing and consistently applying naming conventions and other needed metadata to their short-term records.

D. No more than two years after creation or receipt, users must dispose of a short-term record either by deleting it or by declaring it as a Federal record. A short-term record may be declared "in place" or migrated to an archive appropriate for managing Federal records (see section 05.2).

230.05.2 Federal Records

A. Users must ensure that Federal records are identified and declared as soon as possible, but no later than the two-year timeframe allowed for short-term records. The IGLM team, in conjunction with the I.T. organization, will provide training, guidance and tools to assist users in declaring records in a timely and efficient manner.

B. Information assets qualifying as Federal records in an unstructured data format are declared so as to ensure that:

1) they are maintained in their original "native" format or an approved alternative format with metadata intact; and
2) the appropriate integrity, security and availability controls are in place for the Federal records' required retention periods.

C. Declaring a Record. A user declares a record by identifying and applying, at a minimum, the four types of metadata described below (classification). Additional metatdata may be required depending on the type of Federal record. The minimum metadata requirements are:

1) Business function (from the Large Aggregate Flexible Schedule);
2) A date/time stamp for calculating retention period;
3) The retention period, which includes whether the retention is static (a defined period of time) or dynamic (a defined period of time after a defined occurrence, such as terminating a contract or closing a project file);
4) The office of record for the information asset; and
5) The author or custodian of the information asset.

D. Applying the minimum metadata required for declaring a record is accomplished with the use of either an indexing/archiving application or migrating the record to an archive that requires assignment of the metadata (either manually or automatically). To ensure continued security and availability, Federal records in unstructured data format must be managed using the alternatives described in section 230.05.

E. Classification may occur either manually, quasi-automatically or automatically. Manual classification is performed by users applying the required metadata to property fields for each information asset. Manual classification is the least preferred method due to the potential for error. Quasi-automatic classifiaction may be effected by assigning metadata properties to an EIS. As an example, a SharePoint site may be developed that automatically applies the four classification metadata to any information asset uploaded to the site. Automatic classification may be implemented using UDM system tools developed by the I.T. organization in conjunction with the IGLM team.

230.05.3 Managing and Maintaining Federal Records Using UDM Systems

A. When a Federal record has been declared using UDM Systems, the record is assigned a unique identifier and administratively frozen so that it cannot be altered or deleted (with exceptions outlined in section 06 below) other than through the disposition process.

B. The classification metadata is used to organize and aid in search and retrieval of Federal records within UDM Systems. However, additional metadata such as key words, document title or other information should also be included to aid in searches. The business function taxonomy, retention periods and key words index will be inventoried and maintained by the IGLM team. Changes to the inventory must be documented and approved by the Agency Records Officer.

C. The default status favors availability on at least a "read-only" basis for all users with a business need for access to Federal records in UDM Systems. However, restricted access through permissions management shall be applied as appropriate. This may include but is not limited to restricting access to Federal records containing Personally Identifiable Information (PII), Critical Program Information (CPI), Official Use Only (OUO) and proprietary or other sensitive information. Each office of record, working with the IGLM team, Operational Security (OPSEC), and Infrastructure Administrative Services, must identify information assets in the UDM environment that require restrictions to ensure access is limited only to users who are authorized.

E. To facilitate managing information assets within UDM systems, each office of record must assign a UDM steward to facilitate declaring, classifying, maintaining and disposing of Federal records. UDM stewards will also act as subject matter experts for business function and key words applied to Federal records within UDM systems. UDM stewards also coordinate with the

IGLM team to ensure that Federal records in UDM systems are consistent with the office of record's information asset plan and organizational file outline.

230.05.4 Disposing of Federal Records in UDM Systems

A. Consistent with the requirements of IGLM chapter 11 – Information Lifecycle Management, Federal records in UDM systems shall only be disposed upon meeting their scheduled retention periods according to the Agency File Plan. Auto-delete capabilities shall not be generally implemented within UDM systems except as described in paragraph E of this section. Disposition is a three-part process consisting of eligibility, review and disposition.

B. Eligibility. Eligibility occurs when the scheduled retention period of the Federal record has been met. In UDM systems, this means that a metadata timestamp is applied either manually or calculated based on another metadata field such as declaration date. Each record series from the Agency File Plan includes a means for calculating the eligibility date.

C. Review. When a Federal record has been identified as eligible for disposition, it must be reviewed to ensure that the eligibility requirement has been met, that no exception to eligibility exists (e.g., business need or legal hold), that the means of disposition has been identified (see paragraph D below) and that both the manager of the office of record and the Agency Records Officer have approved the disposition. The approval of disposition may be assigned by the manager of the office of record to the UDM steward. The Agency Records Officer may assign disposition approval to other individuals within the IGLM team.

D. Disposition – General. Upon review and approval of eligible Federal records for disposition, Federal records within UDM systems are either deleted or, in the case of permanent electronic records, offered to NARA. I.T. Infrastructure Adminsitration Services is responsible for the timely deletion from UDM systems of Federal records approved for disposition. The IGLM team is responsible for electronically transferring to NARA approved permanaent Federal records in UDM systems.

E. Disposition – Auto-Deletion. In limited instances, certain record series that typically have a short retention and high volume, may be assigned an auto-delete capability in UDM systems. Implementing auto-delete for any Federal record series requires a business and legal justification memo that is reviewed and approved by both the office of record manager and the Agency Records Officer. Unlike with approval under paragraph C of this section, this approval may not be assigned. The IGLM team will maintain the auto-delete authorization and review it with the office of record on a three-year cycle for changes or terminiation.

F. BPA will comply with OMB Memorandum M-13-12 Open Data Policy – Managing Information as an Asset by regularly reviewing Federal records maintained in UDM systems for their eligibility to be made publicly available based on continuing business value, legal and regulatory obligations and the requirements of section 230.05.3.D of this chapter.

230.05.5 Migration of Records to UDM Environment

The IGLM team and the I.T. Infratructure Administration Services organization are responsible for developing and implementing plans to identify Federal records currently stored in the UDM environment and to migrate those records to UDM systems to comply with the policies of this

chapter. Identification and migration projects will be coordinated with each office of record; sequenced according to risk factors identified for the Federal records; and reviewed on a regular basis by the IGLM Policy Review Board.

230.05.6 Paper Copies of Electronic Records

Crucial metadata, essential for context and the integrity of an information asset in unstructured data format is lost when converted to paper format. Therefore, Federal records created or received in electronic format should generally be kept in native format and paper copies of those records are treated as convenience copies. However, if paper copies contain notes or other markings that provide important context to the material as a Federal record, they must be treated as Federal record material and appropiately managed and maintained. See IGLM Manual chapter 160 for guidance on digitization of paper records.

230.06 POLICY EXCEPTIONS

230.06.1 Administrative Exceptions

The IGLM team and the Infrastructure Adminstrative Services organization will regularly review the collections of Federal records within UDM systems. If Federal records within UDM systems are identified and verified as having incorrect metadata or having been incorrectly declared as Federal records, appropriate corrections may be made administratively as authorized by the office of record, approved by the IGLM team and performed by the Infrastructure Administrative Services organization. All such authorizations, approvals, and actions must be documented and maintained by the IGLM team.

230.06.2 Legal Holds on Unstructured Data

A. As provided for in BPAM 1110 – Use of Government I.T. Equipment, there is no expectation of privacy when using BPA I.T. equipment, even for private use. BPA information assets are government property and may be required to be preserved and produced in litigation; an Inspector General/other audit; or as required for compliance or business purposes. As a result, information assets being maintained in any EIS may have a legal hold placed on them under the authority of the Office of General Counsel (OGC). Legal holds prevent loss through the deletion or alteration of information assets. Information assets in the UDM environment or UDM systems, are retained in their original location and format until the hold is removed.

B. Legal holds are placed by the Cyber Forensics and Intelligence Analysis team ("Cyber Forensics") under the authority of OGC. The user will continue to see the information asset in its original location, but will be unable to delete or alter it, regardless of its retention period. The Cyber Forensics and Intelligence Analysis team may copy information assets in unstructured data format for review and production purposes.

C. In addition to placing legal holds on information assets in unstructured data formats, OGC and Cyber Forensics may also direct that journaling or version controls be initiated on UDM systems or that existing backup tapes of the BPA systems be held and maintained.

IGLM Manual
Chapter 230
Managing Unstructured Data as Information Assets

230.07 RESPONSIBILITIES

A. Unstructured Data Users: All users who create, receive or access information assets in unstructured data format are responsible for determining whether the content of those information assets meets the definition of a short-term record or Federal record and appropriately managing the information asset consistent with the requirements of UDM systems and all applicable IGLM policies.

B. Office of Record: Each office of record is responsible for consistently classifying, organizing and managing its information assets through the information lifecycle in the UDM environment.

C. Office of Record/Organization Managers: Managers are responsible for ensuring information assets within their organization are consistently identified, declared, classified, managed, maintained and disposed of in the UDM environment.

D. Office of Record UDM Steward: The UDM steward for each organization is responsible for coordinating the management of their organizaiton's information assets with the IGLM team and the Infrastructure Administrative Services organization. This includes ensuring Federal records are timely declared and correctly classified consistent with the office of record information asset plan and organizational file outline.

E. Agency Records Officer: The ARO manages the IGLM program for its policy, training, and compliance responsibilities. The ARO reviews and approves/denies requests for exceptions to policies in this chapter including classification, retention, disposition and the taxonomy for UDM Systems consistent with the Large Aggregate Flexible Schedule and Agency File Plan.

F. IGLM Team: The IGLM team has programmatic responsibility for developing policy and guidance on managing information assets in unstructured data format in the UDM environment; training on the policy contained in this and other IGLM Manual chapters as well as Federal regulations; monitoring and auditing UDM by offices of record for compliance; and supporting OGC and the Cyber Forensics team in conducting legal searches, applying legal holds, and addressing e-discovery requirements.

G. I.T. Infrastructure Administration Services: Infrastructure Administrative Services organization is responsible for implementing the IGLM policies of this chapter including retention periods; providing regular reports for compliance purposes; and managing the UDM environment in accordance with the service level agreements that have been developed to ensure appropriate information management standards. The organization shall implement legal searches and holds as required by the Cyber Forensics team and OGC. The organization may assign to the Cyber Forensics team those technical capabilities necessary to conduct legal searches and holds.

H. Cyber Forensics and Intelligence Analysis Team ("Cyber Forensics"): The Cyber Forensics team within the Cyber Security Office is responsible for coordinating with OGC on e-discovery activities including legal search and holds; directing and applying legal holds for UDM systems in coordination with Infrastructure Administrative Services; and collecting and managing materials from the UDM environment that may be relevant to litigation, audits, investigations and other similar forensic activities.

I. Cyber Security Office: The Cyber Security Office is responsible for development, issuance, and enforcement of policy relating to BPA IT Equipment. Cyber Security's governance is based on federal laws, regulations, DOE Orders and BPA guidelines (BPAM 1110 – Use of Government I.T. Equipment).

J. Office of General Counsel: OGC has primary responsibility for e-discovery including directing the scope of legal holds and searchs, and coordinating with the Cyber Forensics team to identify, preserve and collect electronically stored information that may be relevant to litigations, investigations or other e-discovery activities. The Office of General Counsel maintains the list of active litigation as well as lists of those users and resources that are on legal hold. This responsibility cannot be delegated to Infrastructure Administrative Services.

230.08 PERFORMANCE STANDARDS & MONITORING PLANS

A. The IGLM team within Governance and Internal Controls (DGC) and I.T. Infrastructure Administrative Services are the responsible organizations for the performance standards and monitoring plans contained in this chapter.

1) Performance Standards.

- UDM systems technical performance standards are maintained by Infrastructure Administrative Services.
- 99% of Federal records in UDM systems have a complete classification.
- 99% of Federal records in UDM systems identified as being subject to litigation hold have the appropriate hold(s) applied.

2) Monitoring Plans.

- Infrastructure Administrative Services provides annual reports to the IGLM team on:
  - Backups for UDM environment systems [schedules, success/failure data, disposition, use for system recovery].
  - Federal records within UDM systems.
  - General performance of UDM systems in managing and organizing Federal records.

- Performance metrics that are related to policy and Exchange service level agreements.

B. OGC provides the IGLM team and Infrastructure Administrative Services with a list of "Litigation Holds" at least every six months.

C. The IGLM team audits UDM systems and offices of record for compliance with IGLM policies on a three-year cycle by identifying organization based on a risk assessment and performing a compliance review.

230.09 AUTHORITIES & GUIDANCE

List of applicable authorities (statutes, regulations, guidance):

IGLM Manual
Chapter 230
Managing Unstructured Data as Information Assets

Citation	Topic or subject matter
44 USC 2904, 3101, 3102, 3105	Federal Records Act
36 CFR 1235.44 - 50	Requirements for transfer of electronic permanent records to NARA
36 CFR 1236.1 – 6	Subpart A – Electronic Records Management – General
36 CFR 1236.10 – 14	Records Management and Preservation Considerations for Designing and Implementing Electronic Information Systems
36 CFR 1236.20 – 28	Subpart C – Additional Requirements for Electronic Records
OMB Circular A-130	Management of Federal Information Resources

230.10 REVIEW

The IGLM team within Governance and Internal Controls (DGC) is the responsible organization for this chapter. This chapter will be reviewed on a three-year cycle beginning in 2016. All IGLM Manual chapters should be reviewed when revisions are introduced to BPAM chapter 1150 or others governing information management. Editorial updates to the chapter and attachments may be made without Policy Board Review.

230.11 USER PROCESS/PROCEDURES

Training, tools and resources for users to assist in managing information assets in email format are developed and maintained by the IGLM team and can be accessed through the Information Governance website.

230.50 I.T. STANDARDS (RESERVED)

Technical requirements for any UDM system wil be developed in conjunction with the IGLM/Ediscovery project team, the I.T. Project Management Office and I.T. Infrastructure Services.

230.99 REVISION HISTORY

Version	Issue Date	Description of Change	Prepared by
2013-2	11/01/2013	PUBLISHED COMPLETED ORIGINAL CHAPTER	cmfrost