BPA Policy 236-300

Enterprise Data Governance

Table of Contents

1. Purpose & Background

A. This policy provides information governance policies and guidance to comply with the Office of Management & Budget (OMB) Circular A-130, *Management of Federal Information Resources*, and associated regulations on information lifecycle management using an Enterprise Data Governance model. OMB A-130 is derived from several authorities that provide guidance on the wide variety of issues and requirements affecting government information technology and resources. Therefore, this policy is designed to operate in conjunction with additional BPA policies in both the 473 (Information Technology) series and the 236 (Information Governance) series.

B. BPA uses a variety of Structured Electronic Information Systems (SEIS) to create, receive, transform, manage, and maintain its information assets. These systems provide business value through accurate and timely information enabling better decision making; increased productivity, efficiency, and effectiveness of business processes; and fulfilling regulatory and other obligations. To do so, it is important for BPA to maximize the quality, objectivity, utility, integrity, and accessibility of the data and information assets within its SEIS. Additionally, as technology evolves, it is critical that BPA manages its SEIS and the data contained in them to mitigate risks that may accompany new technologies and information processing capabilities.

C. In order to meet regulatory obligations for managing information assets in support of its business processes and mission, and to facilitate BPA's production of information – as required through litigation, Freedom of Information Act (FOIA), or other requests – BPA must implement policies, procedures, and technology standards that will appropriately address structured data management challenges.

2. Policy Owner

The Executive Vice President of Compliance, Audit, & Risk Management has overall responsibility for this policy. The Agency Records Officer within Information Governance develops, implements, and manages this policy on behalf of the Executive Vice President of Compliance, Audit, & Risk Management.

3. Applicability

A. This policy sets requirements for managing BPA's structured data (i.e., data contained in SEIS) as Information Assets and applies to all BPA organizations. Policies governing unstructured data are found in BPA Policy 236-200, *Management of Unstructured Data* (2019).

B. This policy applies to all SEIS created, acquired, licensed, managed, or maintained by BPA and the data and Information Assets contained within them regardless of structure, form, or format.

C. In addition to this information governance policy, all users are responsible for adhering to BPA's policies 473-1, *Acquisition of IT Assets;* 473-2, *Information Technology Policies*; 470-5, *Business Use of BPA Information Technology Services*; 470-6, *Limited Personal Use of BPA Information Technology Services*; 434-1, *Cyber Security Program*; 433-1, *Information Security*; and Privacy Program requirements.

4. Terms & Definitions

4.1 Terms & Definitions

As used in this policy, the following terms and definitions apply:

A. **BPA Dictionary:** A glossary of policy, business, and technical terms/acronyms collected for use as a reference resource for employees throughout the Agency associated with BPA's mission, strategy, and operations.

B. **Data Quality:** The degree to which a set of characteristics of data fulfills requirements. Examples of characteristics are: completeness, validity, accuracy, consistency, availability, and timeliness.

C. **Data Steward:** One who manages another's facts or information to ensure they can be used to draw conclusions or make decisions. They are accountable for specific data categories/domains that alone or in conjunction with other data categories/domains generate information critical to BPA's operations.

D. **Data Stewardship:** The management and oversight of an organization's data as Information Assets to help provide business users with high-quality data that is easily accessible in a consistent manner.

E. **Electronic Information:** Recorded information in electronic form (requiring computer technology to retrieve or access): digital content. This definition includes both the content of the information and associated metadata.

F. **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.

G. **Electronic Recordkeeping System (ERKS):** See Structured Electronic Information System (SEIS); any SEIS that is substantially compliant with the Department of Defense (DoD) Standard 5015.2, *Design Criteria Standards for Electronic Records Management Software Applications*, for integrity, security, and disposition.

H. **Enterprise Architecture:** A strategic model that defines: a) the mission; b) the information necessary to perform the mission; c) the technologies necessary to perform the mission; and d) the transitional processes for responding to changing mission needs including a baseline architecture, a target architecture, and a sequencing plan.

I. **Enterprise Data Dictionary (EDD):** Description of the attributes of a database, together with textual definitions of data elements and objects, as well as physical representation information; a collection of metadata. Many kinds of products in the data warehouse arena use a data dictionary, including database management systems, modeling tools, middleware, and query tools.

J. **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 44 USC § 3301, *Federal Records Act*).

K. **Information:** Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms.

L. **Information Architecture:** The structural design of shared information environments; the art and science of organizing and labelling data and software to support usability and findability. Typically, it involves a model or concept of information that is used and applied to activities and explicit requirements of complex business information systems.

M. **Information Asset:** Recorded information and data that has business value for BPA and must be managed throughout its lifecycle.

N. **Information Asset Plan:** A profile of the organization's information assets by process; documenting the "who, what, where, when and why" of each information asset type, which in turn helps identify business value and management requirements.

O. **Information Owner:** Official with operational authority for specified BPA information (including responsibility for establishing controls for its generation, collection, processing, dissemination, storage, and disposal); generally a business unit manager or designate.

P. **Information System Owner:** An official responsible for the overall procurement, development, integration, modification, or operation and maintenance of one or more cyber systems, including identifying and documenting in the system security plan (SSP): the operation of the information system; unique threats to the information system; and any special protection requirements identified by the information system owner for each information system for which he or she is responsible.

Q. **Interoperability:** The ability of different operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner.

R. **Metadata:** Structured information about any recorded information such as date and time it was created, the author, organization, or other data. This also includes descriptions of content, structure, data elements, interrelationships, indexing and other characteristics of the data, information, and records.

S. **Office of Record:** The organization that, by definition of its mission or function, has primary responsibility for maintenance and retention of the record.

T. **Recorded Information:** Documents, information, and data — including writing, drawing, graphs, charts, photographs, sound recordings, images, and other data or data compilations — stored in any medium from which content can be obtained directly or, if necessary, after conversion into another usable form.

U. **Service Level Agreement:** A contract or memorandum of agreement between a service provider and a customer that specifies, usually in measurable terms, what services the service provider will furnish. Information Technology departments in major enterprises have adopted the idea of writing a service level agreement so that services for their customers (users in other departments within the enterprise) can be measured, justified, and perhaps compared with those of external (sourcing) service providers.

V. **Source of Record:** Document or data, often the original, that is designated as the official copy for reference and preservation; sometimes referred to as the record copy.

W. **Structured Data Management (SDM):** Operational policies, services, and tools that aid in appropriately managing data as information assets in a database or SEIS. SDM are designed to manage structured data throughout the information lifecycle to mitigate risk, to maximize the quality, objectivity, utility, integrity, and accessibility of data, and to enhance the utility and interoperability of SEIS.

X. **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). Electronic Recordkeeping Systems (ERKS) are a sub-set of SEIS that meet additional records compliance requirements.

Y. **System of Record (SOR):** The Structured Electronic Information System that is the authoritative source for a specific data type, element or piece of information. Typically, this is the point of creation or first ingestion into a BPA SEIS. (For the purpose of this policy and not to be confused with *System of Records* as defined in the Privacy Act.)

4.2 Acronyms

As used in this policy, the following acronyms apply:

A. **ACGC:** Agency Compliance and Governance Committee

B. **AIM:** Asset Inventory Management

C. **APSC:** Agency Prioritization Steering Committee

D. **ARO:** Agency Records Officer

E. **BITA:** Bonneville Information Technology Architecture

F. **CRUD:** Create, Read, Update, Delete

G. **DSC:** Data Stewardship Council

H. **DSCWG:** Data Stewardship Coordination Working Group

I. **EDGE:** Enterprise Data Governance Excellence

J. **EDGWG:** Enterprise Data Governance Working Group

K. **EIS:** Electronic Information System

L. **ERKS:** Electronic Recordkeeping System

M. **FOIA:** Freedom of Information Act

N. **IAP:** Information Asset Plan

O. **IGLM:** Information Governance & Lifecycle Management

P. **IGOT:** Information Governance Oversight Team

Q. **IO:** Information Owner

R. **ISO:** Information System Owner

S. **NARA:** National Archives & Records Administration

T. **OMB:** Office of Management & Budget

U. **SDM:** Structured Data Management

V. **SEIS:** Structured Electronic Information System

W. **SLC:** System Lifecycle

X. **SOR:** System of Record

5. Policy

A. BPA shall manage its SEIS and other technology solutions to:

1. Comply with applicable laws and regulations through the use of internal controls;
2. Ensure the integrity, confidentiality, and availability of data as Information Assets within SEIS;
3. Protect BPA's data as Information Assets against internal and external threats; and
4. Support productivity, efficiency, and effectiveness of business processes.

B. BPA, as required by OMB A-130, implements this policy through:

1. Enterprise data governance principles;
2. SEIS scheduling and inventory activities;
3. SEIS and data lifecycle management; and
4. SEIS access and interoperability controls.

5.1 Enterprise Data Governance

SEIS shall be developed, operated, maintained, and decommissioned in a consistent fashion throughout BPA that:

A. Aligns with BPA's mission, priorities, strategy, enterprise architecture, and information architecture;

B. Mitigates risk, supports business processes, and meets regulatory obligations;

C. Incorporates necessary security, confidentiality, privacy, accessibility, and records management capabilities in all SEIS; and

D. Complies with the technical requirements and standards of the Bonneville Information Technology Architecture (BITA).

5.2 SEIS Scheduling and Inventory

A. All SEIS shall have an associated SEIS Schedule that identifies the Information Owner, Information System Owner (or equivalent), and product owner (if appropriate), as well as business and technical Data Stewards. In addition, the SEIS schedule will identify what data and Information Assets are maintained in the system; the means of adding data (inputs) and extracting data (outputs); interoperability with other SEIS; required retentions and disposition; and the data for which the SEIS is the System of Record (SOR). All organizations must include on their Information Asset Plans (IAPs) all SEIS for which they are the Office of Record, including SEIS that they access or they otherwise use.

B. The Enterprise Data Governance Working Group (EDGWG) will regularly review SEIS inventories, schedules, and IAPs to ensure accuracy and compliance with regulations and with BPA policy. In conjunction with the Asset Inventory Management (AIM) system Information System Owner (ISO) and responsible IT personnel, the IGLM team will perform SEIS inspections to validate inventories, schedules, and IAPs. In conjunction with Information Owners and Information System Owners, the Agency Records Officer will authorize changes to SEIS inventories, schedules, and IAPs. The Agency Records Officer will also authorize the disposition of SEIS, their data, and source code in conjunction with SLC processes.

C. BPA maintains a comprehensive inventory of all SEIS that serves as a single source of technical, business, and compliance information as an SEIS profile. Each SEIS profile shall include, but is not limited to:

1. SEIS Schedule;
2. Privacy Impact Assessment;
3. Authority to Operate;
4. System Asset Plan;
5. Key roles (as identified in 5.2.A); and
6. Service level agreements and/or data steward council charters for interoperability and access.

5.3 SEIS Management

A. Management of SEIS and its data is the responsibility of the Office of Record whose business processes the SEIS supports. The manager of the Office of Record is therefore the Information Owner (IO) of the SEIS. Each SEIS shall have a single Information Owner and Information System Owner (ISO) to ensure accountability. In instances where multiple organizations use the SEIS, one organization must be identified as having primary responsibility for the SEIS, with the manager of the organization being the IO.

B. IOs have primary responsibility for the structure and quality of data in the SEIS for which they are the Office of Record throughout the lifecycle of both the data and the system.

C. ISOs have primary responsibility for the technical support and administration of SEIS. Day-to-day maintenance of SEIS and data may be further delegated by IOs and ISOs to Data Stewards. IO and ISO approval is required for changes to the structure, design, data types, access, or interoperability of the SEIS.

D. Both IOs and ISOs shall collaborate throughout the SEIS lifecycle to ensure appropriate operation of the SEIS, as well as management and quality of the data contained in the SEIS.

1. Management of the SEIS Lifecycle. For implementation of new SEIS, IOs, and ISOs shall follow the System Lifecycle (SLC) process as established by the IT Project Management Office (see BPA Policy 473-1, *Acquisition of Information Technology Assets*). Design and development of new SEIS must incorporate documentation of upstream and downstream interoperability through appropriate Service Level Agreements (SLAs) with IOs and ISOs impacted by the new SEIS. Such SLAs will be maintained in the SEIS inventory.
2. Once an SEIS is in production (the Operations and Maintenance, or "O&M" phase), IOs, consulting with ISOs, must monitor the operation of the SEIS. Because the need for and usage of SEIS data may change over time, any such changes must be

implemented so as to ensure the continued quality, accessibility, and use of the SEIS data. Both IOs and ISOs shall make use of "change control" processes to ensure that changes or enhancements to an SEIS maintain the integrity, compliance, and usability of data or information.

3. When the SEIS is approaching the end of its lifecycle, or there is no longer a business need or regulatory obligation for the data, the IO, in consultation with the ISO, must make provisions for the SEIS retirement or decommissioning, including appropriate disposition of the data and source code.

E. **Software-as-a-Service (SaaS) and Cloud Computing:** Where BPA is using SaaS, Cloud Computing, or similar off-premises information technology solutions, an ISO-equivalent may have operations and maintenance responsibilities. In such circumstances, the Information Technology or Transmission Technology manager with responsibility for the designated General Support System shall retain responsibility for review and approval of required documentation associated with the System Lifecycle and I.T. acquisition process. The IO has continuing responsibility for ensuring the ISO requirements of this policy are met, whether through assumption of duties within the IO's organization or through contract with an external provider of operations and maintenance services.

F. **Emergency systems operations:** The Continuity of Operations Plan of an Office of Record must include provisions for assessing SEIS according to business continuity records or legal/financial rights records, for determining required restoration timelines or alternative means of preserving such records. Such plans must be approved by both the Information Owner and Information System Owner of the SEIS (see BPA Policy 236-16, *Essential Records Program*).

5.4 Structured Data Management

A. **Overview:** Standards for data management, consisting of documented, consensus-based agreements on the format and definition of common data, shall be utilized for all SEIS. Data management will use a matrix approach that includes business and technical Data Stewards for each SEIS and domain Data Stewards for groups of data types (e.g. an asset data domain, a person data domain, etc.).

1. **Data Quality and Integrity:** Appropriate controls shall be applied to ensure that data remains accurate, complete, and usable.

2. **Data Compliance:** Data shall remain compliant with the Agency's various obligations including those specified within relevant legislation, Federal and DOE regulations, mandates and policies, and other BPA policies and procedures, as well as other obligations such as contractual requirements.

3. **Data Sources of Record:** To ensure data quality, consistency and interoperability, the Source of Record for specific data or a data types should govern the form and format of all other instances of that data. When considering new systems using

existing data types or new uses of data, IOs/ISOs and Data Stewards must align with appropriate Sources of Record.

B. The Data Stewardship Coordination Working Group (DSCWG) shall define, document, and apply Data Stewardship rules, procedures, and standards to support compliance with this policy. The DSCWG shall review and update its procedures as required but no less often than every three years and shall include the following structured data lifecycle activities:

   1. Creation, collection, input or uploading in an appropriate manner with adequate access provisions and controls to ensure integrity of new data in the SEIS.
   2. Maintenance of data to ensure quality (accuracy and timeliness).
   3. Business rule definition to ensure quality and usage, as well as a Create, Read, Update, Delete (CRUD) roles matrix (see Section 5.5 of this policy).
   4. Transfer of data according to the interoperability requirements of this policy (see Section 5.6 of this policy).
   5. Data sharing agreed to by IOs and ISOs and documented in SLAs that include restrictions (as required by law) on use, disclosure to the public or third parties, and required controls on access, transformation, and disposition.
   6. Disposition of data through enforcement of retention schedules and implemented according to disposition process (eligibility, approval, disposition) including appropriate controls to ensure that data remains available to authorized persons when required.

C. The DSCWG will train and provide guidance for data stewards on data lifecycle management. The DSCWG will also coordinate data management activities among data stewardship councils, IOs, ISOs, and data stewards and serve to resolve issues arising from data quality, system interoperability, and access.

D. To help ensure the quality and consistency of data and information enterprise-wide, BPA utilizes two associated dictionaries:

   1. **BPA Dictionary:** All terms and acronyms included in BPA internal policies will be included in the BPA Dictionary with a citation to the originating policy. Employees may submit additional terms for inclusion as well. Business and technical terms should include, where possible, a citation to the term's originating document or source. The DSCWG reviews terms for inclusion and provide recommendations for BPA Dictionary entries to the Agency Records Officer. As the IO for the BPA Dictionary, the Agency Records Officer is responsible for the design, operation and maintenance, and content of the BPA Dictionary.
   2. **Enterprise Data Dictionary:** The DSCWG coordinates development of data dictionary content and standards, and reviews and approves additions, changes, or deletions to

data elements and objects compiled within the dictionary. As the IO for the Enterprise Data Dictionary, the Chair of the DSCWG is responsible for the design, operation and maintenance, and content of the Data Dictionary.

5.5 Access

A. Access to SEIS

1. IOs/ISOs should consider an accessible and interoperable approach to SEIS while still ensuring the integrity of the SEIS, quality of the SEIS data, and compliance with cybersecurity, privacy, confidentiality, or other requirements.
2. IOs must approve conditions of access (particularly the ability to copy, delete, or manipulate data) for their SEIS. IOs must coordinate with ISOs to provide appropriate support levels of access for users beyond 'read-only.'
3. In addition to access within BPA, certain SEIS may require support of access or interoperability related to users or SEIS that are external to BPA. IOs/ISOs must document external access and interoperability requirements as part of their Authority to Operate (ATO) per BPA Policy 434-1, *Cyber Security Program*.

B. Access rights within SEIS: All SEIS must have clearly defined access/permission roles for CRUD capabilities. CRUD access rights shall include both structure and data. CRUD access may only be approved by IOs or their designated representatives and may only be implemented under the authorization of ISOs.

5.6 Interoperability

A. Interoperability (or the capability of automated data exchange between SEIS) is crucial for supporting BPA business processes. However, interoperability must be weighed against regulatory restrictions on sharing data, ensuring that such interoperability does not compromise data quality, and that the data is not used contrary to the purpose for which it was originally created or collected.

B. Interoperability consists of four types, each of which must be managed according to the characteristics of the SEIS and the needs of its interoperability with other systems:

1. Non-interoperable (or "stand-alone"): SEIS that does not directly exchange data with any other SEIS. All data is either input manually or uploaded from a self-contained data source (e.g., spreadsheet or other End-User Computing Tool (see BPA Policy 230-5, *Internal Controls for End User Computing Tools*).
    a) Stand-alone SEIS must meet records management, cyber security, privacy and other requirements and must have internal controls to ensure data quality. Although not directly interoperable, such systems must also adhere to the requirements of Section 5.4 of this policy.

b) IOs/ISOs must be careful to ensure that any changes to the SEIS resulting in interoperability are managed accordingly. Stand-alone systems shall not be connected to other systems unless a review of structure and data is performed and appropriate changes are made and documented to align the system with the proposed upstream/downstream systems to which it will be connected.

2. Multiple-system interoperability (or "hub-and-spoke"). SEIS that exchanges data with multiple other SEIS that may in turn exchange data with each other or additional SEIS.

   a) In the hub-and-spoke model, the "hub" (typically a data warehouse, data integration layer, etc.) serves as the master SEIS for connecting systems in terms of structure and data.

   b) New SEIS connecting to hub SEIS must conform to the structure and data design of the hub SEIS. In addition, data from external sources must be converted to conforming structures prior to being integrated into a hub and spoke model.

3. Single-system interoperability (or "long-link") is an SEIS that interacts with only one other SEIS either upstream or downstream, but does not transform the data. As a result, such interoperability is not favored because it acts as an alternative means of data flow without adding value. Moreover, such interoperability potentially compromises internal controls and data quality.

   a) There may be instances where regulatory requirements mandate that data move through a long-link system. In such instances, the IO/ISO must provide a business justification to be included in the System Inventory for each SEIS involved.

   b) In instances where the SEIS only interacts with one other SEIS either upstream or downstream, but does transform the data, it shall be treated as a "hub and spoke" system.

4. Complex multiple-system interoperability "spaghetti-map." There are instances where over time, due to lack of controls or other circumstances, systems are connected to other systems through both long-link and hub-and-spoke. Such interoperability is not favored because the complexity of the interactions is difficult to appropriately control for risk, data quality, and data use, as well as having a "cascade effect" on other SEIS.

   a) Spaghetti-map interoperability is not currently prohibited at BPA due to its prevalence. However, for any system changes, when decommissioning and/or replacing SEIS in a spaghetti-map structure, the IO/ISO must provide both a business and technical justification for not re-aligning with a hub-and-spoke structure.

C. In order to ensure alignment among systems in accordance with this interoperability policy, IOs and ISOs should implement SLAs or charter a Data Stewardship council as appropriate based on the type, complexity, risk, business need, and compliance requirements of the SEIS involved.

1. **Service Level Agreements:** For simple interoperability and access between two SEIS, a service level agreement outlining the requirements for moving data (format, timing, and controls) as well as ensuring the requirements of Sections 5.4, 5.5, and 5.6 of this policy are met, must be agreed to and approved by the IOs/ISOs of the respective SEIS. Such SLAs should be reviewed on a regular basis. Changes to the interoperability of SEIS must be documented through updated or new SLAs with the impacted IOs/ISOs, and be included in the SEIS Inventory.
2. **Data Stewardship Councils:** For more complex interactions (e.g., hub-and-spoke or spaghetti-map SEIS configurations), a Data Stewardship council of stakeholders should be chartered with input from the DSCWG. In addition to the functions provided by service level agreements, Data Stewardship councils should consider long-term strategies for underlying business processes, and the use of the data and SEIS involved and act as a forum to resolve issues that may arise from SEIS or data changes. Data Stewardship council charters should be reviewed on a regular cycle or whenever significant changes occur in the interoperability status of the SEIS and/or in the organizations involved.
3. The DSCWG acts as an additional resource for data strategies for implementing service level agreements and as an arbiter for Data Stewardship councils.

D. In addition to interoperability with other BPA SEIS, certain SEIS may require interoperability external to BPA. IOs/ISOs must document external access and interoperability as part of their Authority to Operate (ATO) per BPA policy 434-1, *Cyber Security Program*.

6. Policy Exceptions

A. BPA information assets, data, and SEIS are government property and may be required to be preserved and produced:

1. In litigation;
2. For an Inspector General/other audit; or
3. As required for compliance or business purposes.

The general requirements for disposition of data and decommissioning of SEIS may be suspended for litigation holds, internal audits, investigations, or similar functions.

B. Per BPA Policies 470-5, *Business Use of BPA Information Technology Services;* and 470-6, *Limited Personal Use of BPA Information Technology Services;* there is no expectation of

privacy when using BPA IT equipment, even for private use. As a result, information assets being maintained in any SEIS 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.

C. Legal holds on SEIS are placed by the Cyber Forensics and Intelligence Analysis team (Cyber Forensics) under the authority of OGC. The user may continue to see the SEIS data, 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 structured data format for review and production purposes.

7. Responsibilities

A. **Agency Prioritization Steering Committee (APSC):** Chartered by the Chief Information Officer, the APSC is responsible for IT investment planning, investment controls, and ensuring that IT investments are aligned and prioritized to Agency strategic business objectives.

B. **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 this policy including classification, retention, disposition, and scheduling of SEIS. The ARO, with the AIM ISO, is responsible for BPA's inventory of SEIS and implementing monitoring and compliance with OMB A-130 for SEIS. In this role, the ARO serves on the EDGWG.

C. **Cyber Forensics and Intelligence Analysis Team (Cyber Forensics):** The Cyber Forensics team within the Office of Cyber Security is responsible for:

1. Coordinating with OGC on discovery activities including legal searches and holds;
2. Coordinating with the FOIA Officer on searching collections within SEIS;
3. Directing and applying legal holds in SEIS in coordination with IOs/ISOs for those systems; and
4. Collecting and managing materials from SEIS that may be relevant to litigation, audits, investigations, and other similar forensic activities.

D. **Office of Cyber Security:** The Office of Cyber Security 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 policies.

E. **Data Steward:** Oversees the capture, maintenance, and dissemination of data in SEIS for a particular work or business unit. Data Stewards who write business rules for data are responsible for ensuring the requirements of the Data Governance Policy and Procedures are followed within their unit.

1. **Business Data Steward:** Is accountable for defining, measuring, monitoring, and analyzing an information category/subject area across business functions that is critical to BPA's operations. Business Data Stewards are responsible for documenting and updating business rules for data and to provide them to ISOs and Technical Data Stewards. They are empowered by management to establish procedures within their business functions to create, maintain, and initiate corrective action while balancing their business organizational needs with the needs of the Agency. Business Data Stewards ensure proper change control is applied to data or data definitions and ensure appropriate change control is performed by Technical Data Stewards working on SEIS. Business Data Stewards are liaisons between those responsible for the development or changes in business policies, processes, practices and procedures, the data users, and the Technical Data Stewards. The Business Data Steward reports to the IO for the SEIS and may act on his/her behalf when authorized.
2. **Technical Data Steward:** Is responsible for the safe access, custody, transport, storage of the data and implementation of business rules within SEIS including change control within the SEIS. They are responsible for the technical environment and database structure and as such, act as liaisons between Business Data Stewards and IT functions and support. The Technical Data Steward reports to the ISO and may act on his/her behalf when authorized.

F. **Data Stewardship Coordination Working Group (DSCWG):** Chartered by the IGOT, the DSCWG has programmatic responsibility for developing rules, procedures, and standards for Data Stewardship. The DSCWG is also responsible for coordinating the Data Dictionary, developing and maintaining system SLAs, and training staff on Data Stewardship roles and requirements.

G. **Data Stewardship Councils:** DSCs (which may be identified as "governance boards," "steering committees," or other) are chartered or operate using Service Level Agreements depending upon the complexity of the SEIS interactions involved, but will include Information Owners, Information System Owners, business, technical, and domain stewards, product owners, and other SMEs as stakeholders for SEIS subject to interoperability. They are responsible for ensuring access, interoperability, and data quality, as well as for developing and implementing data use strategies for groups of SEIS. DSCs are also responsible for coordinating change controls, reporting, monitoring, and ensuring adherence of data and systems to the structured data management requirements of this policy.

H. **Enterprise Data Governance Working Group (EDGWG):** Chartered by the IGOT, the EDGWG has programmatic responsibility for developing policy and guidance on managing data in SEIS as information assets; training on the policy contained in this and policies in the 236 series as well as Federal regulations; monitoring and reviewing Offices of Record using SEIS for compliance; maintaining Offices of Record Information

Asset Plans; and supporting OGC and the Cyber Forensics team in conducting legal searches, applying legal holds, and addressing discovery requirements.

I. **Enterprise Architect:** Ensures that the agency's information management and delivery are aligned with the mission and strategy of the enterprise through the development and maintenance of reference models connecting the information that drives the business to the people, processes, and technology, and use these models to identify gaps and make recommendations for changes to the enterprise (business or technology). They also provide standards that will inform policies and principles for information management and delivery.

J. **IGLM Team:** The IGLM team has responsibility for approving records management capabilities for all SEIS, for scheduling SEIS, and for maintaining - in conjunction with the AIM ISO and the Enterprise Architecture organization - the Agency SEIS Inventory.

K. **Information Architect:** The Information Architect plays a key role with IT's data architects and integration architects to ensure that proper planning and implementation of enterprise standards are followed, and promotes and educates customers and stakeholders on the value of enterprise information in support of enterprise architecture. The Information Architect fulfills this role in part by serving on the EDGWG and the DSCWG.

L. **Information Governance Oversight Team (IGOT):** Chartered by the ACGC, the IGOT provides guidance to the EDGWG and the DSCWG and is the forum for escalating policy and compliance issues identified in the data governance program.

M. **Information Domain Steward:** Information Domain Stewards may be established by the DSCWG based on the complexity of data used across multiple business units or the Agency (enterprise) as a whole. The role of an Information Domain Steward is less as "data expert" and more as a facilitator to clarify needs and compliance requirements across business lines and compliance domains. They may become the final authority on business rules or master data when resolution is not possible by the more tactical Functional/Business Data Stewards. The Information Domain Steward is responsible for ensuring change control when data is used across multiple functions or organizations within the Agency. Additional responsibilities may be added as the EDGWG and DSCWG formalize processes and escalation paths for governance processes and data quality.

N. **Information Owner:** An Information Owner must be the manager of the Office of Record for an SEIS and is responsible for ensuring that SEIS and the data/information assets contained within them are consistently identified, declared, classified, managed, maintained, and disposed. The IO may also have responsibility for ISO-equivalent requirements per Section 5.3 of this policy.

O. **Information System Owner:** Manager within the information Technology (J) or Transmission Technology (TT) organization with responsibility for technical support,

operations, and maintenance of an SEIS (see BPA policy 434-1, *Cyber Security Program* for additional responsibilities).

P. **Office of Record:** Each Office of Record is responsible for consistently managing and supporting its data and information assets contained in SEIS throughout the information lifecycle.

Q. **Office of General Counsel:** OGC has primary responsibility for discovery, including directing the scope of legal holds and searches and coordinating with the Cyber Forensics team to identify, preserve, and collect electronically stored information that may be relevant to litigations, investigations, or other 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 Cyber Forensics or other organizations.

R. **Privacy Office:** Is responsible for ensuring that SEIS appropriately limit collection of and ensure security around Personally Identifiable Information (PII) to protect privacy.

S. **Product Owner:** Designated by the Information Owner, the Product Owner is the Office of Record/Organization subject matter expert for the underlying function, business process, and products that an SEIS supports. The Product Owner may develop business rules, controls, or other requirements of an SEIS that serve to ensure data quality and system integration pertaining to the products for which the Product Owner is responsible.

8. Standards & Procedures

Standards and Procedures for this policy will be developed by the EDGWG through 236-300-1, *Enterprise Data Governance Compliance Procedures,* and the DSCWG through 236-300-2, *Enterprise Data Stewardship Procedures*.

9. Performance & Monitoring

A. The IGLM team within Information Governance and the Enterprise Data Governance team are the responsible organizations for the performance standards and monitoring plans contained in this policy.

1. **Performance Standards:**

a) SEIS technical performance standards are maintained by the Office of Record of the system's Information System Owner.

b) Ninety-five percent of new SEIS have a completed schedule prior to 'go live'.

c) The SEIS inventory is 90 percent accurate for SEIS in O&M status.

d) Ninety-five percent of SEIS being decommissioned have an updated SEIS schedule that describes the disposition or transfer of data and source code for the system.

2. **Monitoring Plans:**

a) Annual comparison by IGLM team of SEIS inventory entries to organization Information Asset Plans.

b) Review of SEIS relevant inventory entries against SLC projects through the ITPMO and APSC by the EDGWG.

c) Review of relevant SLAs and DSC Charters by DSCWG for changes in interoperability.

d) Records inspections of SEIS profiles and SEIS operations.

B. The IGLM team reviews SEIS schedules, inventories, and Offices of Record IAPs for compliance with IGLM polices on a three-year cycle by identifying organizations based on a risk assessment and performing a compliance review.

10. Authorities & References

A. 44 USC §§ 2904, 3101, 3102, 3105, *Federal Records Act*

B. 36 CFR § 1236.1 - 6, Subpart A, *Electronic Records Management - General*

C. 36 CFR § 1236.10 - 14, *Records Management and Preservation Considerations for Designing and Implementing Electronic Information Systems*

D. 36 CFR § 1236.20 - 28, Subpart C, *Additional Requirements for Electronic Records*

E. OMB Circular A-130, *Management of Federal Information Resources*

F. DoD Standard 5015.2, *Design Criteria Standards for Electronic Records Management Software Applications*

11. Review

The IGLM team within Information Governance is the responsible organization for this policy. This policy is reviewed on a three-year cycle beginning in 2018. All IGLM policies are reviewed when revisions are introduced to BPA Policy 236-1, *Information Governance and Lifecycle Management,* or other policies governing information management. Editorial updates to the policy and attachments may be made without IGOT and Policy Working Group review and approval.

12. Revision History

Version Number	Issue Date	Brief Description of Change or Review
1.0	12/31/2018	Initial publication
1.1	12/9/2019	Administrative revision. 12/31/2018 effective date not changed. • Term “Data Dictionary” changed to “Enterprise Data Dictionary.” • Added definition of “Source of Record.” • Typos corrected.