BPA Policy 473-1

Acquisition of Information Technology Assets

Table of Contents

1. Purpose & Background

To establish requirements, assign responsibilities, and provide guidance for acquisition of Information Technology Assets within the Bonneville Power Administration (BPA).

BPA's Information Technology organization's overarching mission is to build sustainable partnerships with clients to create Information Technology (IT) solutions for business success, thereby enabling BPA to achieve its potential and mission, and to do so in the most cost-conscious manner. This mission is reliant upon BPA's ability to procure and manage IT assets as efficiently as possible. This includes IT asset lifecycle management from planning, to procurement and implementation, and through sun setting or replacement, ensuring that IT assets adhere to the standards defined by BPA's Chief Technical Officer.

This policy supports, and is consistent with, DOE O 200.1A, Information Technology Management, the statutory and regulatory requirements provided in the Clinger-Cohen Act of 1996 which established the powers and responsibilities of Federal Chief Information Officers, and promotes those principles called out in DOE O 200.1A, specifically:

1. Information Technology Strategic Planning;

2. Capital Planning and Investment Control;

3. Enterprise Architecture;

4. Hardware and Software Acquisition;

5. IT Operations and Use; and

6. IT Contracted Staffing (supplemental and/or professional services that include delivery or development of IT services and assets).

2. Policy Owner

The BPA Chief Information Officer (CIO) is the owner of this policy.

3. Applicability

All organizations and staff within BPA are required to adhere to this policy.

4. Terms & Definitions

A. Asset Management Instructions (AMI) establishes policy for the management and disposition of personal property.

B. Bonneville Purchasing Instructions (BPI), which governs BPA acquisitions made pursuant to this policy, draws on the best purchasing techniques available from both government and commercial sources. It provides for a "best buy" purchasing process which considers quality, timeliness of delivery, quantity, and total costs, including administrative costs.

C. Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers,

storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model, as defined in The National Institute of Standards and Technology (NIST) Definition of Cloud Computing (NIST Special Publication 800-145), is composed of five essential characteristics, three service models, and four deployment models.

1. Essential Characteristics

   a. On-demand self-service

   b. Broad network access

   c. Resource pooling

   d. Rapid elasticity

   e. Measured service

2. Service Models

   a. Software as a Service (SaaS)

   b. Platform as a Service (PaaS)

   c. Infrastructure as a Service (IaaS)

3. Deployment Models

   a. Private cloud

   b. Community cloud

   c. Public cloud

   d. Hybrid cloud

D. Data Subscriptions provide purchased data to the user. Data is unilateral (i.e. information is provided to user). No BPA information is stored, exchanged, or provided to the data source. Subscriptions simply provide purchased data to the user; the provider does not store user modifications or changes to data made by the user or post new data created by the user.

E. Enterprise Architecture (EA) is a strategic information asset base which defines the mission, the information necessary to perform the mission, the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs, and includes a baseline architecture, a target architecture, and a sequencing plan.

F. Federal Risk and Authorization Management Program (FedRAMP) is a government-wide, standardized approach to security assessments and ongoing assessments and authorizations (continuous monitoring). Under the Federal Information Security Management Act (FISMA), Federal agencies must authorize IT service at the agency level. Through Office of Management and Budget (OMB) policy issued 08 December

2011, Federal agencies must use FedRAMP when authorizing cloud services. FedRAMP will assist agencies to acquire, authorize and consume cloud services by adequately addressing security from a baseline perspective.

G. Information Technology (Title 40 US Code, Section 11101), with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—

a) of that equipment; or

b) of that equipment to a significant extent in the performance of a service or the furnishing of a product;

It includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources. All IP-addressable equipment or devices are included in this category.

H. BPA IT Equipment includes but is not limited to BPA's computer networks and any authorized BPA-owned or leased computing device or component that can be attached or connected to BPA's computer network, including any IP-addressable equipment or devices. BPA IT Equipment includes desktop computers and monitors, laptop and portable computers, tablets, thin clients and mobile thin clients, firmware, software, shareware, freeware, personal digital assistants (PDAs), telephones, digital cameras, cell phones, smart phones, facsimile machines, pagers, copiers, photocopiers, printers, scanners, servers, fixed or portable storage devices (e.g. flash drives), routers, peripheral devices, multi-purpose machines (e.g. combined facsimile, printer, and copier), and cloud-based IT services such as Archive-as-a-Service, Storage-as-a-Service, Desktop-as-a-Service, Software-as-a-Service, Platform-as-a-Service, Infrastructure-as-a-Service, Backup-as-a-Service, etc.

I. IT Service, (a sub-component of Information Technology) encompasses several main categories such as managed staffing, managed services, consultant arrangements, and cloud-based services, particularly whenever information is exchanged. In order to distinguish cloud-based services from data subscription, cloud-based services is a software distribution model in which applications are centrally hosted by independent software vendors (ISVs) or application service providers (ASPs) and made available to customers over a network, typically the Internet. Hosted services are a form of cloud-based services in which the vendor runs, manages, and modifies software on behalf of the client and manages the clients' data.   Software as a Service (SaaS) is another form of

cloud-based services in which applications provide the consumer the capability to use the provider's applications running on a cloud infrastructure. The provider manages all aspects of the application, including upgrades.

J. System Lifecycle (SLC) establishes procedures, practices, and guidelines governing Information Technology (IT) strategic planning, asset management, project initiation, concept development, planning, requirements analysis, design, development, integration and test, implementation, operations and maintenance, and disposition of information systems within BPA. One of the key aspects of the SLC is to ensure an orderly and consistent method of developing and deploying systems.

K. IT Acquisition involves any procurement where data or information is developed. This may include but is not limited to procurements of software licenses, computer hardware and equipment, office equipment, such as printers, copiers and faxes, telecommunication systems, cloud services, supplemental and/or professional services that includes development of IT, and any necessary supporting services.

L. Test for Applying Federal Information Security Management Act (TAF) is a process for determining specific applicability of FISMA to all contracting activities, as required by the Chief Operations Officer, in agreement with the Head Contracting Authority, Contracts and Strategic Sourcing and the Office of Cyber Security. Submittal of the TAF, statement of work or quote, to the Office of Cyber Security is required for all acquisitions except as waived by Cyber Security: commercial-off-the-shelf (COTS) software or hardware that will be deployed on-premise at BPA. Completion of the TAF can be performed by the information owner, COTR or other representative from the requesting organization.

5. Policy

A. All planning, budgeting, and acquisition, of IT equipment and services for BPA must be initiated and will be administered by the Office of the Chief Information Officer (OCIO) and shall be processed in a manner consistent with all applicable statutes, regulatory mandates, OMB directives, and Agency requirements. Only IT Managers, or their delegates, under the auspices of the OCIO and the Contracting Officer (CO) may perform the duties of Contracting Officer's Technical Representative (COTR) for IT acquisitions (as defined in section 473.7 Responsibilities). The OCIO will develop standard operating procedures and processes that:

1) Ensure all capital investments, cloud services, and significant enhancements adhere to the Bonneville Information Technology Architecture (BITA) and the SLC.

2) Enable the acquisition of IT equipment and services.

3) Allow use of P-Card to acquire IT equipment and services only when pre-approved in writing by the OCIO after coordination with the Purchase Card Manager.

4) Ensure that a TAF associated with each acquisition is provided to and recorded by the CO, except for internally deployed Commercial-Off-The-Shelf (COTS) hardware

and software, as prescribed by the Office of Cyber Security and the Chief Information Security Officer.

5) Ensure consolidation of package acquisition, volume purchasing arrangements, enterprise-wide agreements and best practices in implementation to take advantage of discount savings.

6) Ensure reallocation of unused IT assets.

7) Track licensing and use of licenses, and help prevent illegal or inappropriate use of IT assets.

8) Ensure all existing and new cloud solutions are compliant with FedRAMP guidance.

9) Ensure IT equipment is managed in accordance with the Asset Management Instructions.

10) Monitor and report compliance to this policy.

6. Policy Exceptions

The following circumstances have been identified as exceptions to this policy:

A. Asset acquisition procedures defined and documented within the Incident Response and Disaster Recovery program shall supersede this policy when such conditions are officially declared by the appropriate authorized governing bodies.

7. Responsibilities

A. Chief Information Officer (CIO)

1. Sponsors and owns this policy, overseeing periodic review of the policy, consistent with BPA strategic and operational plans and all statutory, regulatory, administrative, and OMB requirements. Reports any critical violations of this policy, or the standards and operations procedures referenced in this policy, to the BPA Executive Governance Body.

B. BPA Managers

1. Ensures alignment to policy and engaging IT when business need arises that requires an IT acquisition.

2. Coordinates with IT Managers and Portfolio Managers to document their IT automation requirements in the appropriate IT category sub-portfolio (Office Automation, Application, Datacenter, Agency Information, Cyber Security or Network portfolio).

C. Contracting Officer (CO)

1. Ensures all acquisitions, including but not limited to, IT, IT services, cloud computing services, professional services, commodities, and construction services complete the TAF (with exceptions for internally deployed COTS HW and SW).

2. For all cloud computing services, the CO will work with IT to designate a COTR in the IT Organization.

3. Ensures all agency procurement policies and processes are met.

D. Contracting Officer's Technical Representative (COTR)

1. A designated COTR in the IT organization meeting Supply Chain Services certification requirements who is delegated authority by the Contracting Officer for ensuring performance to the statement of work, and authorization of funds, coordinates with the owner of the asset plan and budget for the IT service, including cloud computing solutions, and all duties as identified in BPI Appendix 14-A.

2. Ensures cloud service provider is FedRAMP certified or ensures a plan is in place to achieve certification.

3. Ensures FISMA determination is included with each procurement request.

4. Develops statement of work and/or specifications for each procurement request and evaluation criteria.

E. Cyber Security

1. Conducts the TAF and makes determination for all acquisitions, including determination of the proper data categorization (FIPS 199), in consultation with the Information Owner and the Information System Owner.

2. Conducts periodic audits to ensure the TAF is completed for all acquisitions.

F. Agency Policy Working Group

1. Oversees authorization, publication, and dissemination of agency-wide policies and policy changes.

8. Standards & Procedures

Applicable standards for BPA IT Equipment are located or referenced within the BITA published on the Chief Technical Officer (CTO) SharePoint site.

System Life Cycle (SLC) processes, procedures, document templates, and examples are published on the CTO's SLC SharePoint site.

Processes and procedures for requesting and completing IT asset acquisitions are published on the IT Help Desk SharePoint site.

9. Performance & Monitoring

On a continuous basis, a delegate assigned by the CIO shall report to the CIO:

A. The number of IT acquisitions performed per P-Card, the sum of dollars spent on those acquisitions, and the individual associated with the P-Card. Sufficient detail shall be retained to identify potential issues with adherence to this policy.

B. The number and magnitude of IT acquisitions recorded in the BES system during the previous six months outside of OCIO purview. Sufficient detail shall be retained to identify potential issues with adherence to this policy.

C. Any exceptions to this policy. Critical violations shall be reported to the BPA Executive Governance Body.

10. Authorities & References

A. DOE O 200.1A, Information Technology Management

B. Clinger-Cohen Act of 1996

C. Federal Information Security Management Act (FISMA)

D. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, The NIST Definition of Cloud Computing

E. Federal Cloud Computing Strategy, 08 Feb 2001, Vivek Kundra, U.S. Chief Information Officer, White House

F. 40 U.S. Code SUBTITLE III: INFORMATION TECHNOLOGY MANAGEMENT

G. Bonneville Purchasing Instructions (BPI)

H. Asset Management Instructions (AMI)

11. Review

This policy shall be reviewed by the policy owner at least every five years for relevant purpose, content, currency, effectiveness, and metrics.

12. Revision History

Version	Issue Date	Description of Change
1.0	5/28/2014	Initial creation.
1.1	5/30/2014	Updated by Lulu Zhang.
1.2	6/17/2014	Updated by Mike Harris and Scott Ducar to emphasize the procurement focus of this policy, improve the definitions, add COTR – IT Manager relationship, and strengthen performance and monitoring requirements.
2.0	8/25/2014	Updated by Mike Harris to include feedback from Supply Chain, PMO, and Program Management.
2.1	8/26/2014	Updated by Mike Harris to include feedback from Damian Kelly RE definition of AMI, use of P-card and AMI in Policy section, and responsibilities of COTR.
2.2	8/26/2014	Updated by Mike Harris to include final polishing from Lynn Mantanona and Scott Ducar RE CO and COTR responsibilities.
2.3	10/10/2014	Updated by Mike Harris to include clarification edits from Jon Wright, Legal Dept. Also provided official policy number of 473-1.
2.4	10/17/2014	Updated by Mike Harris to include suggestions from Diane Cherry (PWG) and Marsha Ard: minor grammatical edits, clarification of the P-Card prohibition, and replacement of AICC.
2.5	11/14/2014	Updated by Mike Harris to include suggestions from Jacilyn Margeson: minor grammatical edits, separation of P-Card use into a discreet element, added reporting responsibility for CIO.

2.6	5/4/2016	Updates to definitions for consistency across policies, by Mike Harris.