U.S Department of Housing and Urban Development (HUD)

Information Technology Asset Management Policy

HUD Handbook 3256.1

July 2023

DOCUMENT CHANGE HISTORY

DATE	VERSION	SUMMARY OF CHANGES	AUTHOR
03/28/2022	1.0	HUD developed a policy on its IT asset management based on Federal mandates (e.g., FITARA and MEGABYTE Act); OMB Category Management Policy and other OMB guidance; and GAO recommendations. The document encompasses total IT asset responsibilities and incorporates existing procedures/directives.	Russell Varnado, OCIO/CTO
10/31/2022	1.0	Revisions to various pages that incorporate comments and feedback from initial OCIO leadership review. Resubmitted for OCIO concurrence.	Russell Varnado, OCIO/CTO
3/24/2023	1.0	Revisions to various pages to incorporate comments and feedback from CISO	Russell Varnado, OCIO/CTO
05/24/2923	1.0	Revisions to various pages to incorporate comments and feedback from Program Offices received under the Departmental Review process	Russell Varnado, OCIO/CTO

Table of Contents

1 BACKGROUND

The U.S. Department of Housing and Urban Development (HUD) acknowledges the need to manage its information technology (IT) assets through an IT Asset Management (ITAM) Program that focuses on the five IT asset lifecycle stages:

- Planning and budgeting,
- Acquisition,
- Deployment and discovery,
- Management and maintenance, and
- Retirement and disposal.

The IT asset lifecycle is a core process of ITAM within an organization. HUD's IT asset management program sets forth ITAM business practices that will join financial, contractual, and asset inventory functions to support lifecycle management and strategic decision making for HUD's IT environment.

The ITAM policy also aligns with the Federal Government's established Category Management approach, which applies to buying and managing goods and services. HUD will apply this approach to IT assets to allow informed and enterprise purchasing solutions for assets. Category Management will assist HUD to eliminate asset and contractual redundancies, increase efficiency, and deliver more value and savings for the ITAM program. Application of ITAM and the category management approach within HUD will involve:

- Identifying core areas of spending
- Collectively developing heightened levels of expertise
- Leveraging shared best practices
- Providing acquisition, supply, disposal, and demand management solutions
- Analyzing the IT Asset Portfolio

1.1 Scope and Objectives

This document describes the formal Information Technology (IT) policy for ITAM that complies with federal and HUD regulations, policies, and guidance. The primary objective of this policy is to correct a lack of formal, centralized ITAM capabilities, including hardware asset management (HAM) and software asset management (SAM). The lack of a formal ITAM program has resulted in a reactive approach that has led to higher IT costs, a marginalized ability to negotiate with IT vendors, a higher risk of licensing agreement violations, and an increase in the likelihood of a cyber intrusion and exploitation to HUD's networks, application and data.

This policy provides guidance and direction for HUD for managing all Information Technology (IT) assets, including all software, hardware, mobile, telecommunications, and cloud assets. This document outlines the business rules and guidelines for consistently procuring, implementing and executing HUD's ITAM program processes and procedures for managing IT software and IT hardware throughout all lifecycle phases of an IT asset.

2 PURPOSE

This document sets forth the ITAM Policy. This policy establishes an ITAM program that will implement systematic processes to join contractual, financial, inventory, risk management, security, and IT governance functions to support (1) management of IT assets throughout their lifecycles and (2) guide strategic decision-making for the HUD's IT environment.

3 RESCISSION

This policy does not rescind any other policy or document. This is HUD's IT Asset Management Policy, version 1.0. This document will be reviewed annually, and rescission information will be updated as necessary.

4 APPLICABILITY

The IT Asset Management Policy is applicable to all HUD organizations, HUD employees, IT contractors, and other stakeholders using IT assets or having roles and responsibility for hardware and software asset management, oversight, and successful day-to-day operations of HUD's IT applications and systems.

5 EFFECTIVE IMPLEMENTATION DATE

This policy is effective immediately upon the date of approval.

6 IT ASSET MANAGEMENT POLICY

All HUD IT assets shall be managed in accordance with Federal regulations, Office of Management and Budget (OMB) requirements, Cybersecurity & Infrastructure Security Agency (CISA) Binding Operational Directives, National Institute of Standards and Technology (NIST) standards and guidance, and HUD IT policies and procedures. This policy establishes the framework and guidelines for managing information technology (IT) assets throughout their lifecycles and includes the following activities:

A. Implement a centralized ITAM program that complies with federal IT Asset regulations and guidance and establishes a baseline inventory of all assets purchased, deployed, used or disposed across the Department.

B. Identify ITAM requirements that align with HUD's IT Strategic Plan[1].

C. Act in a fiscally responsible manner to identify and optimize IT asset costs required to perform mission and business functions in the most efficient manner that adds the most value.

D. Implement centralized ITAM processes and services around the five ITAM lifecycle stages: (1) planning and budgeting; (2) acquisition; (3) deployment and discovery; (4) management and maintenance; and (5) retirement and disposal. ITAM monitoring of asset

[1] http://hudatwork.hud.gov/HUD/cio/po/i/stratplan

consumption must trigger contract changes related to the removal of unused or underutilized assets, as well as changing technology, vendor, and internal requirements.

E. Incorporate ITAM governance within the Configuration Change Management Board (CCMB) that enforces ITAM life cycle processes to implement effective decision making and incorporate into existing standards, processes, and metrics where possible.

F. Utilize automated ITAM tools, as resources become available, to maintain, track and analyze ITAM data.

G. Ensure the IT asset management life cycle processes include clearly defined roles and responsibilities, proper governance and controls, and integration points with other IT processes.

H. Maximize the use of acquisition vehicles developed by OMB's Federal Strategic Sourcing Initiative to acquire commodity IT, and only use non-standard Department-wide IT solutions based on an alternative analysis that demonstrates the technology benefits and/or provides better value and is validated and approved by the Technical Review Sub-Committee (TRC) (for project technical designs) and CCMB (for IT product approval). Where HUD uses a governmentwide acquisition vehicle to acquire IT, it will perform an independent assessment of the IT's compliance with Section 508.

I. Analyze asset usage and other data to make cost-effective decisions, and informed IT resource planning, budgeting, and future acquisitions. ITAM monitoring of asset consumption should trigger contract changes related to the removal of unused or underutilized assets, as well as identifying contract requirements for addressing changing technology, vendor, and internal requirements.

J. Ensure that in the planning and budgeting phase all current and planned IT assets are associated with one or more IT systems or applications, are clearly identified, associated with the appropriate phase requirements, and associated with an investment in the HUD's IT portfolio (i.e., are associated with the appropriate unique investment identifier (UII) listed on the Department's IT Portfolio Summary submitted to OMB).

K. Actively manage vendor relationships and control vendor contracts and associated IT work requirements, relationships, and performance for the efficient delivery of contracted products and services; minimize potential business disruption and drive the most value from vendors. All communications with vendors shall be conducted in accordance with the current HUD Vendor Communication Plan[2]. Contract management will be conducted in accordance with HUD Acquisition Regulation (HUDAR[3], Part 2401 of the Federal Acquisition Regulation System).

[2] https://www.hud.gov/program_offices/cpo

[3] https://www.hud.gov/program_offices/cpo/hudar

L. Perform all software acquisitions in accordance with Federal and HUD Acquisition Regulations, the Making Electronic Government Accountable By Yielding Tangible Efficiencies Act of 2016 (MEGABYTE Act of 2016), Federal Category Management guidance[4], the Federal Financial Accounting and Reporting[5] requirements related to IT assets, Security of the Software Supply Chain through Secure Software Development Practices[6], and the Federal Information Security Modernization Act of 2014 (FISMA)[7].

M. All ITAM associated acquisition documentation shall be retained in a centralized contract repository (Purchase Request Information System Management (PRISM)) accessible only to those personnel with the appropriate roles and responsibilities.

O. Acquire only IT assets contained in the HUD TRM and the standardized list of technologies and versions approved for use in the HUD non-production and production environments to avoid purchasing duplicative technologies. Requests for new technologies or non-standard assets must comply with HUD's CCMB[8] process for new products, alternatives, and limited use requests.

P. As HUD's IT funds are available, HUD will invest in additional and/or more advanced asset management tool(s) to support core lifecycle processes.

Q. Establish comprehensive IT asset inventories by identifying and collecting information using automated discovery and inventory tools. Any tool and process used for software asset management must specifically collect information about software license agreements and track and maintain identified software licenses to control assets throughout the asset management lifecycle.

R. Assess current IT asset inventories and usage and establish controls to ensure the maximum use of IT equipment, installed software, and services (i.e. ensure that HUD needs and is using all IT assets that the agency is paying for), as required to manage and deliver the required assets to address changing business requirements within established costs and schedule.

S. Maintain comprehensive IT asset data by tracking all assets from purchase to retirement and disposal, including data collected at integration points with quality management, software engineering, change management, and information security management processes.

T. Right-size the number of IT devices (e.g., mobile phones, smartphones, desktop and laptop computers, personal tablets, etc.) issued to employees, consistent with the Telework Enhancement Act of 2010, operational requirements (including continuity of

[4] https://www.acquisition.gov/gsam/subpart-507.71

[5] https://files.fasab.gov/pdffiles/2022_%20FASAB_%20Handbook.pdf

[6] https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

[7] https://www.cisa.gov/federal-information-security-modernization-act

[8] http://hudatwork.hud.gov/HUD/cio/po/i/it/sd/devlife/def/CCMB/ccmb

operations, and initiatives designed to create efficiency through the effective implementation of technology.

U. Follow HUD established policies, directives, and procedures, to ensure hardware and software are approved for installation by the CCMB and TRC, tested through the HUD Test Center before deployment, and added to the asset inventory. HUD shall ensure proper procedures are in place for the removal of unauthorized assets.

V. Create and maintain a configuration management database (CMDB) which will serve as a mechanism to track information system configuration items (i.e. hardware, software, databases, etc.), ownership, and asset interdependencies.

W. Promote further efficiencies in IT by evaluating and leveraging appropriate government-wide or Department-wide IT solutions that consolidate activities such as desktop services, email, and collaboration tools.

X. Provide training, and as required, relevant certifications to Software License Managers (SLM) and Hardware Asset Managers (HAM) to improve understanding of legal and compliance requirements, including what is expected of users with regard to the protection of intellectual property rights.

Y. Develop, maintain, and communicate to end users the ITAM policy, processes and procedures, and their integration with other policies and processes that support the management of IT assets and services.

Z. Ensure that the SAM and HAM lifecycle processes have integration points with configuration and change management processes (i.e., a change to a platform may affect licensing).

AA. Monitor the performance of the ITAM program and software assets by developing compliance reports (reporting, at a minimum, the compliance position of managed software through proper SLM) and by developing key performance indicators (KPIs) which quantify the success of the ITAM program.

BB. Ensure that IT assets receive timely patches and are securely configured and version-controlled in compliance with underlying contracts.

CC. Ensure that all HUD employees and contractors are informed of and comply with the Departmental Rules of Behavior for Use of Information Resources[9] and OMB Circular A-130. Unauthorized use of a user account or a computing resource is a violation of 18 U.S.C. § 1030, Fraud and related activity in connection with computers, constitutes theft and is punishable by law. Users will be held accountable for their access and use of HUD

[9] https://www.hud.gov/sites/documents/RULESOFBEHAVIOR.PDF

computing resources as described within the Departmental Rules of Behavior for Use of Information Resources and the system and application rules of behavior.

DD. Per HUD Handbook 2400.25 IT Security Policy and HUD Handbook 3252.1 Software Configuration Management Policy, HUD employees and contractors shall not acquire or implement any unauthorized hardware or software for any internal or external HUD system or application or place any unauthorized software on any HUD computing device. All trial or promotional software will be restricted to test environments for the purpose of evaluation and determination by HUD that the software is approved and placed on the software allowlist.

EE. Adhere to FAR Part 42[10], "Contract Administration and Audit Services," in the event of a government audit of a vendor. An audit response team shall be formed and follow the guidance of the Office of General Counsel (OGC) Procurement Law Division and the applicable Contracting Officer (CO). The audit response team shall appoint a single point of contact (POC) for all communications with the vendor conducting the audit and immediately notify all HUD personnel to cease any/all communications with the vendor.

FF. Comply with HUD property management policy[11] and other hardware and software procedures regarding tracking and managing assets that have reached the "end of life" or usability. In addition, all assets associated with the retirement and decommissioning of an IT system or application must adhere to HUD's established IT system decommissioning and disposal processes.

7. ROLES AND RESPONSIBILITIES

7.1 Chief Information Officer (CIO)

A. Establish an ITAM program within the Office of the Chief Information Officer (OCIO) that includes executive sponsorship and governance.

B. Designate a Departmental software license manager (SLM) to manage all Department-wide software agreements and licenses.

C. Define an ITAM policy, process, and procedures to include automated, repeatable processes to aggregate hardware and software asset management and maintenance requirements and associated funding, as appropriate, for associated acquisitions.

D. Ensure effective implementation of ITAM processes that include continuous diagnostics and mitigation (CDM) capabilities for HUD and integration with the ITAM program and tools. The processes should include a means to discover and review existing assets that are currently in use against the HUD's approved list of products and provisions for

[10] https://www.acquisition.gov/far/part-42

[11] https://www.hud.gov/program_offices/administration/hudclips/handbooks/admh/2235.7

identified products not on the approved list (i.e., consider whether to add the product to the approved list or identify an approved alternative to replace it).

E. Enforce the establishment and maintenance of a Departmental inventory of IT hardware and software assets, including a comprehensive inventory of all software licenses purchased, deployed, and in use.

F. Monitor and manage ITAM expenditures for hardware and software (including subscription services and Software as a Service (SaaS)) throughout the asset life cycle phases.

G. Enforce compliance with software license agreements, consolidation of redundant applications and license requirements, and identification of other cost-saving opportunities.

H. Ensure ITAM staff are sufficiently trained to carry out the duties of IT asset management and software license management.

I. Ensure the establishment of goals and objectives for the IT asset management and SLM programs.

J. Review and approve all IT acquisition strategies and acquisition plans that include IT assets. For contract actions that contain IT assets that are outside of an approved acquisition strategy or acquisition plan, the CIO shall review and approve the action itself (e.g., procurement actions for alternatives or exceptions when existing approved solutions do not meet a business need).

K. Ensure that a Departmentwide process is in place to ensure that all acquisitions that include IT assets are reviewed by OCIO staff and are:

   i. Led by personnel with appropriate Federal acquisition certifications, including specialized IT certifications, as appropriate;

   ii. Reviewed for opportunities to leverage acquisition initiatives such as shared services, category management, strategic sourcing, and incremental or modular contracting and use such approaches, as appropriate;

   iii. Supported by cost estimates that have been reviewed by the CIO;

   iv. Adequately implementing incremental development as necessary to accommodate IT asset requirements; and

   v. Determined to comply with Section 508 and HUD’s Section 508 policy.

7.2 Chief Technology Officer (CTO)

A. Integrate ITAM program requirements within the CCMB and TRC governance processes and procedures to ensure uniform and consistent enforcement of this policy and communications with executive leadership.

B. Ensure ITAM resource requirements are identified and prioritized.

C. Ensure proper coordination and seamless process flows with related programs and services within OCIO (i.e. cybersecurity, enterprise architecture, infrastructure support, etc.).

D. Establish ITAM program performance metrics to monitor overall effectiveness and efficiency of the ITAM process and procedures.

E. Provide ITAM communications and identify training requirements to all stakeholders, including end users, ITAM program staff, contracting officer representatives (COR), system owners (SO) and information system security officers (ISSO).

F. Monitor compliance with relevant IT Asset Federal mandates, OMB policy, and HUD policy and procedures.

G. Develop and implement a vendor management strategy that includes processes to improve relationships with suppliers and support the development of IT sourcing strategies.

H. Maintain the Technical Reference Model (TRM)[12], the list of technologies and the version(s) approved (allowlist) for the current production environment, the legacy technologies that should be retired/decommissioned, as well as determine future technologies that align with the target architecture and IT/IM strategic plan and roadmap.

7.3 Configuration Control Management Board (CCMB)

A. The CCMB Chair will have overall ITAM governance responsibilities related to policy compliance and standards.

B. Manage and maintain the CCMB limited use process for determining if a technology or version should be added to the TRM and allowed into the production environment.

C. Manage the CCMB-approved product list (allowlist) and publishes the certified products for use on HUD's production environments on the CCMB Portal.

[12] https://csrc.nist.gov/glossary/term/technical_reference_model#:~:text=Definition(s)%3A,of%20service%20components%20and%20capabilities.

D. E. Manage the list of disapproved products (denylist) as required for Supply Chain Risk Management requirements.

7.4 Infrastructure Operations Office (IOO)

A. Manage and coordinate all aspects of the ITAM program with standard operating procedures.

B. Manage the Enterprise Software Initiative (ESI) that includes:

   i. Further enhance the Department’s procurement oversight process by ensuring that proposed procurement actions (i.e., commercial software contracts, agreements, and interagency agreements) meet Department and programmatic needs and expectations and that the documentation adequately supports the proposed procurement.

   ii. Provide oversight of enterprise software initiatives.

   iii. Provide strategic feedback on strategic sourcing strategies in all categories (including IT), such as leveraging government-wide acquisition vehicles and enterprise-wide agreements and contracts.

C. Access the Department wide IT hardware and software management system established as the HUD CMDB. The CMDB will contain all HUD hardware inventory, infrastructure configuration information, Commercial Off-the-Shelf (COTS) entitlements, and software implementation metrics.

D. Assure IT asset inventory information is associated and/or synchronized to provide the complete picture of the IT asset lifecycle between the CMDB, acquisition purchasing databases, financial databases, and any other systems requiring an authoritative data source for IT asset information.

E. Manage HUD infrastructure operations, asset discovery, and scanning capabilities to verify and validate IT assets using available tools and services, including the federal wide Continuous Diagnostics and Monitoring Program .

F. Take the appropriate steps to immediately remove any IT assets that are not approved by the CCMB and notify the CCMB Chair of these actions via email to the CCMBRequests@hud.gov mailbox.

G. Oversee and manage operational configuration management requirements, which includes application testing, application registration, infrastructure operational monitoring, and release management.

H. Implement appropriate security controls that comply with both federal and HUD policies and guidance to secure information system assets.

I. Provide guidance and support to HUD Headquarters and Regional customers in managing IT hardware and software assets.

J. Review all enterprise IT hardware assets at least once a year.

K. Determine if IT is obsolete[13], still meets user requirements or needs modification. Further, determine if IT hardware is unused or underutilized to comply with E.O. 13589, Promoting Efficient Spending. After replacement, obsolete IT hardware assets will be coordinated for disposal in accordance with HUD's property management procedures.

L. Identify software that does not have the required/current licenses, research and assemble proof-of-purchase, and request replacement licenses from publishers, as needed. Any software found to be noncompliant with software license agreements must be addressed in a plan of action and milestone (POA&M) to reach compliance within 120 days.

7.5 Software License Manager (SLM):

A. Serve as the Departmental lead for implementation of ITAM software management, federal regulations, and HUD policies.

B. Lead Departmentwide efforts, working in collaboration with the Chief Procurement Officer staff and other organizations, as appropriate, to centralize license management, implement strategies to reduce duplication, and ensure the adoption of software best practices.

C. Manage, through policies and procedures, all Department wide commercial and COTS software agreements and licenses.

D. Employ a centralized SAM procedure that includes the development of an approved list of software and an associated implementation plan. This plan should address, at a minimum, the lifecycle phases, funding aggregation and other considerations, including the use of SaaS.

E. Lead an evaluation of software products in the HUD IT environment to validate that they continue to meet both business and technical requirements and submit the results to the CCMB for review.

F. Increase the use of Government-wide software licensing agreements and implement strategies to reduce duplication of products.

[13] Information Technology (IT) products reach the end of their life cycle (obsolesce) for various reasons, including market demand, innovation in technology, inability to source critical components, substitution by functionally superior technology, or deviation in vendor's business direction.

G. Ensure, through the review of software contract information, that terms and conditions in Department commercial license agreements are consistent with best ~~business~~ practices to the maximum extent practicable and are negotiated to meet the Department's needs.

H. Ensure that the personnel involved in SAM (e.g., legal, acquisition, system administration, technical support, and users (as appropriate)) are trained in relevant software management topics, such as intellectual property and software contracts, license negotiations, license compliance laws, regulations, software audits, security planning, configuration management, provisional services (i.e., SaaS), and compliance with Section 508 of the Rehabilitation Act of 1973, as amended (*29 U.S.C. § 794d*).

I. Develop and implement an assessment and approval process to determine the cost and benefit of purchasing software maintenance programs. The process should include a means of assessing operational impacts and risks, including information security and privacy as described in OMB Circular A-130 and other related OMB guidance.

J. Use software policies, processes, and procedures to comply with supply chain guidance and prevent software piracy and theft.

K. Participate in federal category management efforts to remain knowledgeable about available governmental and Department-wide acquisition vehicles which facilitate HUD's effort to centralize purchasing.

L. Develop and oversee the Department's software management centralization plan in an effort to centralize license management, implement strategies to reduce duplication, and ensure the adoption of software management best practices.

M. Review and coordinate all software license requirements and consolidate non-enterprise software inventories.

7.6 Hardware Asset Manager(s)

A. Implement and build controls for the hardware inventory that maintains visibility into hardware asset processes and build controls for hardware assets throughout the lifecycle to maximize value, provide data on hardware assets to support customer demand, maintenance and operations, and strategic decision-making.

B. Develop, implement, and promote policies, processes, and procedures for hardware asset acquisitions, installations, usage, and disposition.

C. Manage, through policy and procedure, all hardware assets.

D. Remain knowledgeable of all available Federal and Department-wide acquisition vehicles for IT hardware and facilitate HUD efforts to centralize purchasing.

7.7 Domain Managers

A. Manage the assigned domain in accordance with the delegated authority granted to each domain manager.

B. Comply with all policies and procedures related to the functions of the domains.

7.8 Section 508 Coordinator

A. Provide technical advice and assistance to offices to ensure that information and communications technology (ICT) meets Section 508 standards.

B. Provide technical advice and assistance to Department users related to assistive technology.

C. Perform ICT Section 508 reviews, testing and provide recommendations to improve Section 508 compliance.

7.9 IT Project Managers and Program Managers

A. Manage project tasks, resources, schedules, and costs for IT projects in compliance with HUD's IT Asset Management policy.

B. Assist the System Owner with the operation and maintenance of the information system and compliance with HUD's IT Asset Management policy.

C. Coordinate with the System Owner to ensure all the information system related documentation such as Project Planning and Management documentation, security plans, system inventories, configuration management plans (GSS and Major Applications), etc. are updated as needed and in compliance with HUD's IT Asset Management policy.

7.10 Enterprise Architecture

A. Coordinate with the CTO and IT governance, to develop the target architecture and information technology/information management (IT/IM) strategic plan and roadmap to achieve the optimal, cost-effective IT portfolio to best support the Department's mission.

B. Coordinate with the ITAM Program staff to ensure IT assets align with target enterprise architecture.

C. Coordinate with SLM to identify potential cost savings opportunities and identify programmatic IT opportunities to reduce spending.

7.11 Office of Information Technology Security (OITS)

A. Support the CIO with the management and oversight of HUD's information security program.

B. Monitor compliance with Departmental IT security policy and IT security control catalog guidance, and procedures for all HUD systems and associated IT assets.

C. Participate in CCMB reviews and conduct security impact assessments for all requests submitted for CCMB disposition.

D. Conduct security assessment of systems prior to deployment in the production environment to ensure appropriate security and privacy controls are implemented to protect HUD assets.

E. Provide guidance to Program Offices on cybersecurity requirements and the catalog of security and privacy controls for protecting organizational operations and systems assets.

7.12 Information System Security Officers (ISSO)

A. As the principal point of contacts (POCs), oversee the security of information systems including all security aspects of their assigned system(s) from inception through disposal, as well as ensuring system availability.

B. Ensure security and privacy controls for securing HUD system(s) belonging to the Program Office are in place, effective, and comply with HUD's established policies for IT Asset security controls, IT security control catalog, and IT Asset Management.

7.13 Office of the Chief Procurement Officer (OCPO)

A. Directly supports the ITAM program by establishing policies, processes, and procedures to ensure that the acquisition of all IT assets comply with federal Supply Change Risk Management guidance and OMB Category Management Policies and principles throughout HUD while ensuring that the Department's mission goals are met.

B. Establish and oversee the process for analyzing all expenditures under category management and report progress to the SLM as required and in accordance with OMB-issued guidance.

C. Ensure contracts do not restrict or prohibit the sharing of all prices, terms, and conditions for commercial and COTS software licenses with other Government entities, including posting said information on the Acquisition Gateway.

D. Ensure that HUD does not initiate contract actions or interagency agreements that include IT unless they are reviewed and approved by the OCIO and are consistent with the acquisition strategy and acquisition plan previously approved by the OCIO.

E. Ensure IT contract actions are communicated and tracked with the Software License Manager, Hardware Manager, ESI, and Enterprise Architecture as required throughout the procurement process.

F. Ensure that all software acquired complies with Section 508.

7.14 Business and IT Resource Management (BIRM)

A. Ensure IT investments and acquisitions are reviewed for alignment with the approved IT Asset standards established by the CCMB.

B. Provide guidance to Program Offices on IT capital planning and acquisition procedures that comply with this policy.

C. Coordinate with the ITAM Program to identify potential IT savings and IT portfolio consolidation through strategic plans and implementation.

7.15 System Owner (SO)

A. Ensure documentation is provided for each business system and application that includes an inventory of all associated hardware and software assets.

B. Ensure full implementation and compliance with all HUD policies, directives, and procedures related to procurement, deployment, operation, and maintenance for the information system(s) under their purview.

C. Ensure lifecycle costs, including IT assets, and other system sustainment funds are budgeted and maintained throughout the life of the information system(s) managed.

D. Develop a full lifecycle plan for any hardware or software of their information system(s) based on the vendor’s established life expectancy of the product and total cost of ownership. Any new or existing product that will reach end-of-life (EOL) within three years and is part of a Component IT System will require the development of remediation, upgrade, replacement and funding plan to remove the EOL item(s) from the Component’s environment completely within that time frame. A plan of action and milestone (POA&M) shall be submitted for risk acceptance to the Component ISSO and AO to track remediation milestones appropriately.

E. Ensure incident, vulnerabilities, or other weaknesses found with the IT system (including the hardware and software system components and operating environment) are identified and tracked via POA&Ms and properly addressed in collaboration with the ISSO.

F. Ensure HUD information system hardware and software inventories are updated as changes occur to the information system.

8 AUTHORITIES

This policy implements the following federal requirements and mandates for IT assets throughout the asset lifecycle:

- Public Law 104-106, commonly referred to as the Clinger-Cohen Act of 1996
- E-Government Act of 2002 Public Law 113-291—Dec. 19, 2014: Title VIII National Defense Authorization Act For Fiscal Year 2015, Subtitle D, commonly referred to as the Federal Information Technology Acquisition Reform Act (FITARA)
- Making Electronic Government Accountable by Yielding Tangible Efficiencies (MEGABYTE) Act of 2016, 40 U.S.C. 22301, Public Law 114–210, July 29, 2016
- Rehabilitation Act of 1973, section 508, 29 U.S.C. 794d, Electronic and information technology[14]
- 44 U.S.C. Chapters 31, Records Management by Federal Agencies[15], and 35, Coordination of Federal Information Policy[16]
- Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource[17]
- Federal Accounting Standards Advisory Board, Statement of Federal Financial Accounting Standards (SFFAS) No. 10. Account for Internal Use Software[18]
- OMB M-15-14, Memorandum for Heads of EXECUTIVE DEPARTMENTS AND AGENCIES: Management and Oversight of Federal Information Technology, June I 0, 2015
- OMB Category Management Policy, issued in a series of memoranda:
  - M-16-02, “Category Management Policy 15-1: Improving the Acquisition and Management of Common Technology: Laptops and Desktops,” dated October 16, 2015
  - M-16-12, “Category Management Policy 16-1: Improving the Acquisition and Management of Common Technology: Software Licensing,” dated June 2, 2016

[14] https://www.govinfo.gov/content/pkg/USCODE-2011-title29/html/USCODE-2011-title29-chap16-subchapV-sec794d.htm

[15] https://www.archives.gov/about/laws/fed-agencies.html

[16] https://www.govinfo.gov/app/details/USCODE-2021-title44/USCODE-2021-title44-chap35

[17] https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

[18] https://files.fasab.gov/pdffiles/handbook_sffas_10.pdf

    - M-16-20, “Category Management Policy 16-3: Improving the Acquisition and Management of Common Technology: Mobile Devices and Services,” dated August 8, 2016

- OMB M-16-21, Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software, August 8, 2016

- OMB M-19-13 “Memorandum for The Heads of Departments And Agencies, Category Management: Making Smarter Use of Common Contract Solutions and Practice, March 20, 2019

- National Archives and Records Administration (NARA) Records Schedule provides mandatory instructions to maintain Department’s operational records and the process to disposition[19]

- Executive Order 14028, Improving the Nation’s Cybersecurity, May 12, 2021

- National Institute of Standards and Technology (NIST) SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, May 2022

- NIST SP 800-53r5, Security and Privacy Controls for Information Systems and Organizations, September 2020

- Information Technology Security Policy, HUD Handbook 2400.25, August 5, 2020

9. REFERENCES

- Public Law 111-292, commonly referred to as the Telework Enhancement Act of 2010

- Executive Order 13589, “Promoting Efficient Spending,” dated November 9, 2011

- Executive Order 13103, “Computer Software Piracy,” dated September 30, 1998

- OMB Circular A-131, “Value Engineering,” revised December 2013

- OMB Category Management Policy, issued in a series of memoranda, including, but not limited to,[16] the following:

    - M-16-11, “Improving Administrative Functions Through Shared Services,” dated May 4, 2016

    - M-15-14, “Management and Oversight of Federal Information Technology,” dated June 10, 2015

[19] https://www.archives.gov/records-mgmt

    - M-14-03, “Enhancing the Security of Federal Information and Information Systems,” dated November 18, 2013

    - M-13-02, “Improving Acquisition through Strategic Sourcing,” dated December 5, 2012

    - M-12-10, “Implementing PortfolioStat,” dated March 30, 2012

- “Digital Government: Building a 21st Century Platform to Better Serve the American People,” dated May 23, 2012[20]

- “2019 Federal Cloud Computing Strategy”[21]

- Office of Federal Procurement Policy (OFPP) memorandum, “Transforming the Marketplace: Simplifying Federal Procurement to Improve Performance, Drive Innovation, and Increase Savings,” dated December 4, 2014[22]

- OFPP memorandum, “’Myth-Busting”: Addressing Misconceptions and Further Improving Communication During the Acquisition Process,” dated May 7, 2012[23]

- OFPP memorandum, “Myth-Busting 3”: Further Improving Industry Communication with Effective Debriefing” dated January 5, 2017[24]

- OFPP memorandum, “Myth-Busting #4” Strengthening Engagement with Industry Partner through Innovative Business Practices, May 2, 2019[25]

- U.S. Government Accountability Office (GAO) GAO-14-413 “Federal Software Licenses—Better Management Needed to Achieve Significant Savings Government-Wide,” issued in May 2014

- Federal Acquisition Regulations (FAR), including, but not limited to, the planning provisions established in FAR Subpart 7.1, “Acquisition Plans”; Part 10, “Market Research”; and Part 15, “Contracting by Negotiation,” and the post-award provisions in Part 42, “Contract Administration and Audit Services.”

[20] https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html

[21] https://cloud.cio.gov/strategy/

[22] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/procurement/memo/simplifying-federal-procurement-to-improve-performance-drive-innovation-increase-savings.pdf

[23] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/procurement/memo/myth-busting-2-addressing-misconceptions-and-further-improving-communication-during-the-acquisition-process.pdf

[24] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/procurement/memo/myth-busting_3_further_improving_industry_communications_with_effectiv....pdf

[25] https://www.whitehouse.gov/wp-content/uploads/2019/05/SIGNED-Myth-Busting-4-Strenthening-Engagement-with-Industry-Partners-through-Innovative-Business-Practices.pdf

- NIST SP 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations.

- The Federal Property and Administrative Services Act of 1949, Section 202(b), amended.

- Public Law 84-863, Section 2, Budget and Accounting Procedures Act of 1950, as amended.

- Federal Managers' Financial Integrity Act of 1982, 31 U.S.C. 3512, Executive agency accounting and other financial management reports and plans, subparagraphs (a)(2)(B) and (C).

- Title 41, Public Contracts and Property Management, Subtitle C, Federal Property Management Regulations System[26]

- 5 CFR, Part 2635, Office of Government Ethics.

- 48 CFR, Chapter 1, Federal Acquisition Regulation (FAR) System, Part 45.

- 41 CFR, Chapter 101, Public Contracts and Property Management

- Stevenson-Wydler Technology Innovation Act of 1980, as amended (15 U.S.C. 3710(i) et seq.).

- Personal Property Management, HUD Handbook 2235.7[27]

- HUD IT Security Policy, HUD Handbook 2400.25[28]

- Software Configuration Management Policy, HUD Handbook 3252.1[29]

10 DEFINITIONS

Auto-Discovery Tool - Applications that can audit computers and services for physical and software configuration information.

Allowlist - An approved list or register of entities that are provided a particular privilege, service, mobility, access or recognition.

Denylist - A list of discrete entities that have been previously determined to be associated with malicious activity.

Commercial Off-The-Shelf (COTS) Software - Software developed, tested, and sold by commercial companies to the general public. This software meets operational

[26] https://www.ecfr.gov/current/title-41/subtitle-C/chapter-101
[27] https://www.hud.gov/program_offices/administration/hudclips/handbooks/admh/2235.7
[28] https://www.hud.gov/program_offices/administration/hudclips/handbooks/cio/2400.25
[29] https://www.hud.gov/program_offices/administration/hudclips/handbooks/cio/3252.1

requirements without modification or alteration to perform on a HUD network or computer. Examples include word processors, databases, application generation, drawing, compiler, graphics, communications, and training software.

Configuration - The generic term used to describe a group of configuration items that work together to deliver an IT service or a recognizable part of an IT service. Configuration is also used to describe the parameter settings for one or more configuration items.

Configuration management - The technical and administrative activities concerned with the creation, maintenance, and controlled change of configuration items throughout the life of a product.

Configuration Management Database (CMDB) - A database that contains all relevant information about the components of the information system used in an organization's IT services and the relationships between those components. Typically includes hardware, software, and topology information.

Contractor - A company or institution that is under contract to the government and from whom a program manager expects to receive a delivered system as specified in a contract. A contractor may also be a vendor.

Cost - Defined in Statement of Federal Financial Accounting Concepts No. 1, "Objectives of Federal Financial Reporting," as the monetary value of resources used. Cost is defined more specifically in Statement of Federal Financial Accounting Standards (SFFAS) No. 4, "Managerial Cost Accounting Concepts and Standards for the Federal Government," as the monetary value of resources used or sacrificed or liabilities incurred to achieve an objective, for example, to acquire or produce a good or to perform an activity or service. Depending on the nature of the transaction, the cost may be charged to operations immediately (i.e., recognized as an expense of the period) or to an asset account for recognition as an expense of subsequent periods. In most contexts within SFFAS No. 7, "Accounting for Revenue and Other Financing Sources," "cost" is used synonymously with "expense."

Cost savings – The reduction in actual expenditures to achieve a specific objective, as defined in OMB Circular A-131.

Documentation - Records required to plan, develop, operate, maintain, and use electronic records and software. Included are systems specifications, file specifications, codebooks, record layouts, user guides, and output specifications.

Enterprise License - Allows the purchasing organization to use multiple copies of a specific COTS software program, usually up to a specified number, across the organization for a set price as a more cost-effective acquisition strategy than the purchase of individual copies.

Hardware - (1) The generic term dealing with physical items as distinguished from its capability or function such as equipment, tools, implements, instruments, devices, sets, fittings, trimmings, assemblies, subassemblies, components, and parts. The term is often used in regard to the stage of development, as in the passage of a device or component from the design stage into the hardware stage as the finished object. (2) In data automation, the physical equipment or devices forming an IT system and peripheral components. See also software.

Hardware Asset Management (HAM) - The process of tracking, monitoring, and reporting the physical components of computers and computer networks from acquisition through disposal to provide a comprehensive inventory of hardware assets within the IT infrastructure.

Hardware asset manager - An individual responsible for managing, through policy and procedure, all IT hardware assets and for implementing hardware asset management best practices to track and monitor hardware assets throughout their lifecycle.

Information system – A discrete set of IT, data, and related resources (such as personnel, hardware, software, and associated IT services) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, in accordance with defined procedures, whether automated or manual.

Information technology (IT) - Defined as follows:

- The term "information technology" includes any services or equipment, or the interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency, where such services or equipment is considered "used by an agency" if it is used by the agency directly or if it is used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.

- The term "information technology" 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 provisioned services such as cloud computing and support services that support any point of the lifecycle of equipment or services), and related resources.

- The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require the use of the equipment.

IT asset - An IT item of value to stakeholders. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., data, information, software, capability, function, service, or intellectual property). The value of an asset is determined by stakeholders in consideration of loss concerns across the entire system life cycle. Such concerns include but are not limited to business or mission concerns. ***Note**: Assets are the lowest level at which IT is planned, acquired,* *implemented, and operated. All IT hardware and software shall be associated with the comprising system/investment and tracked and monitored throughout their lifecycles in accordance with the HUD's ITAM processes.*

IT investment - The expenditure of IT resources to address mission delivery and management support. An IT investment may include a project or projects for the development, modernization, enhancement, or maintenance of a single IT asset or group of IT assets with related functionality and the subsequent operation of those assets in a production environment. *Note: Each investment is assigned a unique investment identifier (UII) for tracking, budgeting, and reporting purposes (both internally and externally to OMB).*

IT service management (ITSM) - The implementation and management of quality IT services that meet the needs of the business. IT service providers perform ITSM through an appropriate mix of people, processes, and information technology. See also "service management."

Life Cycle Management - 1) The management of a system or item, starting with the planning process and continuing through successive management processes and associated life-cycle management phases and associated milestones, until a system is terminated. (2) A management process applied throughout the life of an automated information system that bases all programmatic decisions on the anticipated mission-related and economic benefits derived from the life of the automated information system.

Maintenance - Any act that either prevents the failure or malfunction of an asset or restores its operating capability. It includes inspection, upgrading, testing, servicing, and classification as to serviceability, repair, rebuilding, and reclamation.

Network - Two or more computers connected to each other through a multi-user system or by other electronic means to exchange information or share computer hardware or software.

IT Program / Project Manager (ITPM) - The designated individual with responsibility for, and authority to accomplish, program objectives for development, production, and sustainment to meet the user's operational needs. The PM shall be accountable for credible cost, schedule, and performance reporting to the appropriate governance bodies.

Software - (1) A set of IT assets programs, procedures, and associated documentation concerned with the operation of an IT system (i.e., compilers, library routines, manuals, circuit diagrams). (2) The programs, procedures, rules, and any associated documentation pertaining to the operation of data processing systems.

Software asset management (SAM) - the process of tracking, monitoring, and reporting the use and ownership of software assets throughout their lifecycle, including licenses, versions, and installed endpoints. SAM is part of an overall service and configuration management process.

Software License Management (SLM)— The proactive approach to SAM that enables accurate procurement and deployment of software licenses based on contract entitlements, product use rights, and actual usage.

System Component - A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware.

Vendor management – The practice of actively managing relationships with vendors to develop, manage, and control vendor contracts, relationships, and performance for the efficient delivery of contracted products and services; minimize potential business disruption, and drive the most value from vendors.