SMG 3210.4

FDA STAFF MANUAL GUIDES, VOLUME III - GENERAL ADMINISTRATION

INFORMATION RESOURCES MANAGEMENT

INFORMATION TECHNOLOGY MANAGEMENT

INFORMATION TECHNOLOGY HARDWARE ASSET MANAGEMENT POLICY

Effective Date: 09/10/2019

1. Purpose
2. Background
3. Scope
4. Policy
5. Responsibilities
6. Supersession
7. References
8. Effective Date
9. History

1. PURPOSE

The purpose of the Food and Drug Administration's (FDA) Hardware Asset Management (HAM) policy is to reduce IT spending and support cost, improve IT governance, operation and security while ensuring compliance with the Federal Information Technology Acquisition Reform Act (FITARA) (found in the National Defense Act of 2015), the HHS Logistics Management Manual (LMM), and the Federal Acquisition Regulation – Property Clauses.

FDA's HAM function manages IT resources in such a way that FDA knows what IT assets it owns, where they are physically and logically located, who uses them, what services they support, what it costs to purchase, use, and retire them, under what contracts they were purchased and are maintained, when they are scheduled to be retired, and all other information that allows FDA to effectively manage its hardware assets.

The goal of the HAM policy is to enable a consistent and systematic approach to the management of hardware assets while improving budget, asset, acquisition and technology data.

2. BACKGROUND

The Clinger-Cohen Act of 1996 was passed to compel Federal organizations to be fully accountable for economic and efficient management of IT and directed agencies to establish a Chief Information Officer (CIO) position specifically for that purpose.

To be in compliance with the Act, the Agency requires that investments in IT be managed in such a way that the hardware assets associated with them are tracked in terms of cost, use, and location from the time they are ordered to the time they are retired. The basic activities of IT asset management are as follows:

- Plan – Plan and define the purpose, scope, objectives, policies and procedures, and the organizational and technical context or IT asset management.

- Identify – Select and identify the structure for all the infrastructure configuration items (CIs), including their owner, their interrelationships, and configuration documentation. It includes allocating identifiers and version numbers for CIs, labeling the items, and entering them in the IT asset management database.

- Control – Ensuring that only authorized and identifiable CIs are accepted and recorded from receipt to disposal. This ensures that no CI is added, modified, replaced, or removed without appropriate controlling documentation; e.g. an approved change request, and an updated specification.

- Account – The reporting of all current and historical data concerned with each CI throughout its lifecycle. This enables changes to CIs and their records to be traceable, e.g. tracking the status of a CI as it changes from one state to another, ‘under development’, ‘being tested’, ‘live’, or ‘withdrawn’.

- Verify and Audit – A series of reviews and audits that verify the physical existence of CIs and check that they are correctly recorded in the IT asset management system.

- Incident Management – The IT asset management database is used by the IT Help Desk to confirm, troubleshooting and research assets associated with incidents.

- Problem Management – The IT asset management database is used by problem management personnel to help identify and correct root causes of incidents over time.

- Change Management – The IT asset management database is kept up to date through the change management process. In turn, the IT asset

- management database can be used to determine what IT assets should be changed, based on their age, performance, and incident history.

- Release Management – The IT asset management database is used to determine what IT assets should be replaced, upgraded or retired when a new release is implemented.

- Capacity Management – The IT asset management database serves as the primary input for capacity modeling. In turn, capacity management identifies IT assets that may be causing performance problems and predicts the IT assets that will be needed to handle expected workload in the future.

In Information Technology Service Management (ITSM) literature (formerly IT Infrastructure Library or ITIL), asset management "is the process responsible for tracking and reporting the value and ownership of financial assets throughout their lifecycle…(and) part of an overall service asset and configuration management process.[1]

All hardware assets belong to the Agency per current laws and regulations, are managed by the CIO appointed Hardware Asset Manager and supporting teams. The hardware inventory is inclusive of all IT equipment within the Agency obtained by any means included approved contract vehicles, pCard purchases or acquired via inter-agency transfer.

3. SCOPE

FDA's IT HAM effort covers the following aspects of FDA's IT infrastructure that handles data, voice, and video:

- Servers – The FDA-owned or controlled server hardware and middleware, and their major components

- Networks – The FDA-owned or controlled servers, routers, switches and cables and their major components

- Storage Devices – The FDA-owned or controlled storage units, such as Storage Area Networks, and their major components

[1] ItSMF International, The IT Service Management Forum, 2007; Foundations of the IT Service Management Based on ITIL V3; Van Haren Publishing; p.324

- Desktops/Laptops – The FDA-owned or controlled personal computers, workstations, tablets, and laptop computers, both within and outside of FDA spaces

- Mobile Devices – The FDA owned or controlled cellular mobile devices, both within and outside of FDA spaces

This policy does not apply to the following:

- Scientific equipment – Although scientific components are considered hardware assets and included in Property Management Information System(PMIS), they will be out of scope at this time.

- Personnel – People are not tracked under IT asset management; they are managed by the FDA personnel management system

- Personnel environment – The environment in which people, rather than IT assets, reside is not tracked under IT asset management; it is managed by the FDA facilities organization

4. POLICY

The following requirements must be followed for managing hardware assets at the FDA. This should be done for each organization within OIMT.

- Procurement Request – Hardware asset purchases must follow FDA procurement policy and procedures including due diligence of market research. Market research is a continuous activity and is required for exercising options as well to determine whether the exercise is in the best interest of the Agency, or if another solution of vehicle is more appropriate. The Master Approved Technologies (MAT) list should be reviewed prior to any attempt to procure IT equipment. IT equipment must not be purchased unless it has been reviewed and approved by IT Security and is on the MAT List. eOrder is the preferred method of ordering IT equipment that is approved via the established Blanket Purchase Agreement approved by the Office of Acquisitions and Grants (OAGS.)

- Intake Request – Current IT intake processes require review for redundancies with current business capability and compatibility with existing architecture. The goals of these processes include reducing redundancies of purchases of similar products, achieving economies of scale in purchase vehicles, ensuring legal requirements in usage and lifecycle, and reducing support cost associated with the technology footprint. These factors will affect whether a requested product is added to the MAT list. Inclusion on the MAT list is not approval for acquisition, which is a separate process. The hardware procurement request process should be followed after an item is added to the MAT list.

- Deployment, Installation and Management– Only approved FDA owned or leased hardware assets may be installed within the FDA environment, and only by authorized personnel in accordance with IT policy and procedures. All equipment installed must also account for ongoing operations, maintenance and support. The procuring party and/or the designated business owner is responsible for ensuring adequate funding is provided for these activities for the entire lifecycle.

- Inventory Management – Per HHS mandate, all HHS OP/STAFFDIV's will use (PMIS) to track accountable hardware assets. Within PMIS, HHS tracks two categories of property (hardware assets) – "accountable," defined as personal property with a value of $5,000 and greater, and "sensitive," which is defined as personal property with a value of less than $5,000 that is deemed sensitive in nature. GSA defines sensitive as "all items, regardless of value, that require special control and accountability due to unusual rates of loss, theft, or misuse, or due to national security or export control considerations." For both accountable and sensitive property, HHS must track the asset for the life of the asset until final disposition. This includes any and all intervening transfers, defined as the movement of the asset within an OP/STAFFDIV or between STAFFDIVs and OPDIVs. At a minimum, accountable IT equipment will be inventoried on a yearly basis through the Personal Property management Office (PPMO) and coordinated with the Center Property Officers.

- Hardware Audits and Validation – FDA will conduct periodic audits and validations of hardware assets.

- Disposal of Hardware Assets – Hardware assets are to be disposed of in an appropriate manner. State, Local, HHS, and FDA guidelines must be followed. Prior to disposal of IT equipment, the appropriate Center Property Officer should be contacted for guidance.

- Monitoring – FDA performs scans that detect hardware use and monitor compliance. Unauthorized usage is subject to removal and other existing policies. The business owner is responsible for remediating all issues detected.

- Training – All personnel that handle hardware assets must be trained in relevant management topics. This includes PMIS and other HHS hardware asset related courses.

5. RESPONSIBILITIES

FDA Chief Information Officer (CIO) - The FDA CIO has the overall responsibility for FDA IT resources, appointing the Hardware Asset Manager, developing a governance structure for managing hardware assets and managing the IT environments.

Hardware Asset Manager - The Hardware Asset Manager has responsibility for the HAM program, ensuring compliance with this policy and is supported by multiple teams across the Agency.

Property Management Officers - Property Management Officers are responsible for the management and control of all personal property assigned to a Center/Office. In this role, they manage the day-to-day handling of personal property, tracking, maintaining, and documenting property from acquisition to disposal within the Property Management Information System (PMIS).

FDA Office of Acquisitions and Grants Services (OAGS) - OAGS is responsible for dedicated IT Acquisition personnel and for streamlining acquisitions in accordance with FITARA and Federal Acquisitions Regulation (FAR).

FDA Configuration Manager (CM) - CM is responsible for maintaining relevant hardware and model categories in the CMDB.

Personal Property Management Office (PPMO) - The PPMO is responsible for ensuring that the Agency meets its fiduciary, legislative and procedural obligations, in accounting for and safeguarding all personal property items.

Inventory Order Management Team – Manages the ordering of IT equipment for the FDA.

Center IT Liaisons – Provides oversight for Center IT purchases and policies.

Property Management Team (PMT) – Manages the initial distribution and disposal of IT equipment for the FDA.

6. SUPERSESSION

This policy is in effect until declared void by the FDA CIO or superseded by subsequent policy approved by the FDA CIO.

7. REFERENCES

Federal Information Management Acquisition Reform Act (FITARA)

HHS Logistics Management Manual Policy and Procedures

Federal Acquisitions Regulation – Property Clauses

Federal Information Security Management Act (FISMA) of 2002

HHS Enterprise Performance Lifecycle, (EPLC), 2008

8. EFFECTIVE DATE

The effective date of this guide is September 10, 2019.

This SMG will be reviewed and updated as necessary to ensure alignment with FDA strategies, policies and priorities.

9. Document History – SMG 3210.4 “Information Technology Hardware Asset Management Policy”

STATUS (I, R, C)	DATE APPROVED	LOCATION OF CHANGE HISTORY	CONTACT	APPROVING OFFICIAL
Initial	12/11/2006	N/a	Strategic IT Programs, OCIO, HFA-82	Kathleen Heuer, FDA Chief Information Officer (Acting)
Revision	09/05/2019	N/a	Division of Business Partnership and Support	FDA Chief Information Officer (Acting)