DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

AFMAN17-1203_AFGM2020-01
2 NOVEMBER 2020

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: SAF/CN
1800 Air Force Pentagon
Washington, DC 20330-1800

SUBJECT: Department of the Air Force Guidance Memorandum to AFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM)*

By Order of the Secretary of the Department of the Air Force, this Air Force Guidance Memorandum immediately changes AFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM)* 18 May 2018. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications; the information herein prevails, in accordance with DAFI 33-360, *Publications and Forms Management*.

AFMAN 17-1203 rewrite completed SecAF Air Force Directive Publication Reduction initiative May 2018. However, new updates are required to bring the publication compliance. The purpose of this AFGM is to fill the gap in policy.

This Memorandum becomes void after one year has elapsed from the date of this Memorandum, or rewrite of AFMAN 17-1203, whichever occurs earlier**.**

Lauren Barrett Knausenberger, SES, DAF
Deputy Chief Information Officer

Attachment
AFMAN17-1203, Information Technology Asset Management
AFMAN 17-1203_AFGM2020-01

(Replace) OPR: SAF/CNSC
(Replace) Certified by: SAF/CNS (Col Terrence Adams)

(Replace) This Department of the Air Force Guidance Memorandum (AFGM) implements Air Force Policy Directive (AFPD) 17-1, *Information Dominance Governance and Management*, and supports AFPD 17-2, *Cyberspace Operations* and AFPD 10-6, Capabilities Requirements Development. This AFGM provides the overarching guidance and direction for managing AF Information Technology (IT) hardware and software. This AFGM is applicable to all civilian employees and uniformed members of the Regular Air Force, United States Space Force, the Air National Guard, and the Air Force Reserve. The authorities to waive wing/unit level or Space Force equivalent requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See DAF Instruction (DAFI) 33-360, Publications and Forms Management, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. The use of a name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Department of the Air Force. Compliance with attachments 2, 3, and 4 is mandatory.

Chapter 1
Information Technology Asset Management

1.1. General Overview. This AFGM has three chapters and provides guidance and direction for operational management of IT hardware and software assets and defines specific roles, responsibilities and processes.

Overall, Information Technology Asset Management (ITAM) is defined as a framework and set of processes, polices and material solutions that provide efficiency, legal and contractual licensing compliance, financial accountability and inventory management. To comply with ITAM requirements outlined on this AFGM, technologies and techniques for continuous network monitoring and automatic tracking of hardware and software assets will be used to the maximum extent possible in place of manual physical inventories. Organizations must continue to use manual inventories and procedures for hardware or software that cannot be accounted for with automated tracking techniques due to assets not installed, not configurable as discoverable, or not connected to a monitored network. **(T-1).**

1.2. Roles and Responsibilities.

1.2.1. Deputy Chief Information Officer (SAF/CN).

1.2.1.1. SAF/CN is the lead office to establish and implement all ITAM policy, processes and requirements. **(T-0)**.

1.2.1.2. Develops strategy, policy, and guidance for ITAM of IT hardware and software.

1.2.1.3. Resolves management issues and policy disagreements between Major Commands (MAJCOMs), functional managers, and non-Air Force agencies for IT hardware and software assets.

1.2.1.4. Identifies, reviews, approves, and forwards formal ITAM training requirements to Headquarters Air Education and Training Command.

1.2.1.5. As the functional manager, designates the Accountable Property System of Record (APSR) to support ITAM accountability. The current designated APSR is the Defense Property Accountability System (DPAS), further defined in **Attachment 2**.

1.2.1.6. Ensures primary Accountable Property Officers (APO) are appointed as needed. **(T-0)**.

1.2.1.7. Requires APOs to be appointed in writing at appropriate level. **(T-0)**.

1.2.1.8. Designated as the official with the responsibility of executing of Enterprise Agreements (EA).

1.2.2. Chief, Special Access Program (SAP) Information Technology and Support (SAF/CNSZ).

1.2.2.1. Air Force Special Access Programs (SAP) IT hardware assets will not be tracked in DPAS. SAP IT hardware assets will be tracked separately within SAP configuration control project databases in coordination with Security, Special Program Oversight and Information Protection (SAF/AAZ) as the primary OPR for SAP assets. **(T-0)**.

1.2.3. Deputy Chief of Staff, Intelligence, Surveillance, Reconnaissance and Cyber Effect Operations (AF/A2/6).

1.2.3.1. The AF/A2/6 is the Department of the Air Force lead for systems in Air Force Sensitive Compartmented Information Facilities (SCIFs), Air Force Sensitive Compartmented Information (SCI) systems, and national-level intelligence, surveillance and reconnaissance systems in accordance with DODI 5200.01, *DOD Information Security Program and Protection of Sensitive Compartmented Information (SCI)*, AFPD 17-2, *Cyber Warfare Operations*, AFMAN 14-403, *Sensitive Compartmented Information Security and Intelligence, Surveillance, and Reconnaissance Systems Cybersecurity and Governance*, and AFI 17-130, *Cybersecurity Program Management*.

1.2.3.2. Air Force IT hardware assets under the control of AF/A2/6 will be tracked in the designated APSR, or other approved accountable systems of record for accountability of hardware, as designated by Air Force/A2/6. **(T-0)**.

1.2.3.3. The Air Force Chief Intelligence, Surveillance, and Reconnaissance (ISR) Information security officer will evaluate all security issues and concerns before directing how Air Force SCI and ISR assets will be tracked. **(T-1)**.

1.2.3.4. AF/A2/6 will provide guidance for meeting regulatory compliance for IT hardware assets not tracked in the designated APSR. **(T-0)**.

1.2.3.5. AF/A2/6 IT requires automated asset and license management, accomplished via system configuration, network management, license management and IT service management tools and processes that together facilitate total lifecycle asset management of both physical and virtual assets to enable compliance with Office of the Director of National Intelligence (ODNI) *Improving Cybersecurity for the Intelligence Community Information Environment Implementation Plan*, Aug 19. **(T-0)**.

1.2.4. Assistant Secretary of the Air Force, Acquisition, Technology and Logistics (SAF/AQ).

1.2.4.1. Sets acquisition requirements to support Integrated Life Cycle Management within the Department of the Air Force. **(T-1)**.

1.2.4.2. As the Air Force Service Acquisition Executive (SAE), ensures contracting activities are performed in accordance with laws and statutes. **(T-0)**.

1.2.4.3. Executes SAE responsibilities outlined in DOD guidance for execution of Department of the Air Force acquisitions. **(T-0)**.

1.2.4.4. Ensures programs, to include modifications, are properly defined and justified in budget documentation. **(T-0)**.

1.2.4.5. Executes Title 10 United States Code Section 2464, *Core logistics capabilities*, and Title 10 USC § 2466, *Limitations on the performance of depot-level maintenance of materiel.* **(T-0)**.

1.2.4.6. Ensures implementation across acquisition programs for compliance with core and organic requirements. **(T-0)**.

1.2.4.7. Assigns Program Executive Officers (PEOs) to programs per DODI 5000.02, *Operation of Adaptive Acquisition Framework*. **(T-0)**.

1.2.5. Air Combat Command (ACC).

1.2.5.1. Is the service owner for Enterprise IT.

1.2.5.2. Serves as lead for implementation of ITAM program for IT Hardware and SW.

1.2.5.3. Publishes software entitlements, implementation and ITAM account inventory metrics.

1.2.5.4. Manages the Air Force Evaluated/Approved Products List (E/APL) and publishes to the Air Force Portal the certified commercial-of-the shelf (COTS) Software Products for use on Air Force networks.

1.2.5.5. Coordinates with SAF/CN, Air Force/A2/6, Air Force Materiel Command (AFMC) and MAJCOMs for software license requirements and consolidates non-enterprise software agreements.

1.2.5.6. Identifies and forwards formal ITAM training requirements to SAF/CN.

1.2.5.7. Surveys, consolidates, validates, and tracks all MAJCOM, Field Operating Agency (FOA), and Direct Reporting Unit (DRU) requirements for potential Air Force enterprise software licenses for COTS software.

1.2.5.8. Recommends candidate software products for potential Air Force-wide or DOD-wide licensing to the applicable AFMC product center designated with the responsibility for procurement of enterprise licenses as the purchasing agent.

1.2.5.9. Serves as the Air Force software license manager to review and consolidate the Air Force software license inventory. MAJCOM and base inventories include locally owned software and software not yet transferred to an enterprise software license agreement.

1.2.5.10. In coordination with AFMC, designates a product center as the OPR for managing the Air Force Enterprise Software License Program or establishing DOD-wide enterprise software license agreements.

1.2.5.11. Ensures all COTS license requirements are purchased using approved Air Force Enterprise License Agreements (ELAs), Joint Enterprise License Agreements JELAs, DOD Enterprise Software Initiative (ESI) or other approved DOD/Air Force/Intelligence Community (IC) contract vehicles. **(T-0)**.

1.2.5.12. With input from the Software Enterprise Acquisition Management Lifecycle Support (SEAMLS) office and IT Business Analytics Office (IT BAO) offices, makes determination if new software products should be considered for new ELA/JELA and provide recommendations to SAF/CN. **(T-1).**

1.2.6. MAJCOM, DRU, FOA, or Equivalent.

1.2.6.1. Air Force Equipment Control Officer (AFECO) will be the Functional Equipment Control Officer (FECO) for the MAJCOMs. For DRU, FOA, or equivalent, appoint a FECO when this role is not designated by a previous memorandum of agreement (MOA) or memorandum of understanding (MOU). Document acknowledgement of duties with handwritten or digital signature. **(T-1)**.

1.2.6.2. Notifies AFECO via email at AFECO@us.af.mil when the FECO changes.

Chapter 2

HARDWARE ASSET MANAGEMENT

2.1. Scope.

2.1.1. The scope of IT hardware asset management encompasses business processes related to the asset management lifecycle including acquisition, receipt and acceptance, physical inventory, transfer, management, disposal, and financial reporting.

2.1.2. IT hardware is a subset of the General Equipment (GE) Assessable Unit (AU), where IT hardware assets owned by the Air Force are captured within the general ledger and reported on the financial statements.

2.2. IT Hardware Definition and Types.

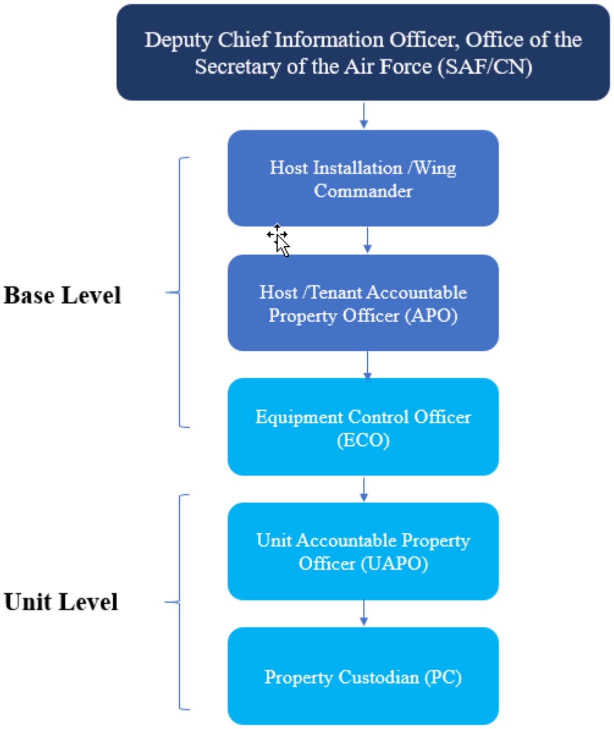
2.2.1. IT Hardware refers to devices such as computing systems and/or network systems that process, store, and distribute data. This includes but is not limited to computers, displays, network equipment, printers/scanners, and servers. To determine if an IT hardware asset meets the criteria to be tracked within DPAS, refer to **paragraph 2.4**.

2.2.2. IT hardware typically utilizes software and firmware. Software and firmware are covered within **Chapter 3.**

Chapter 3.

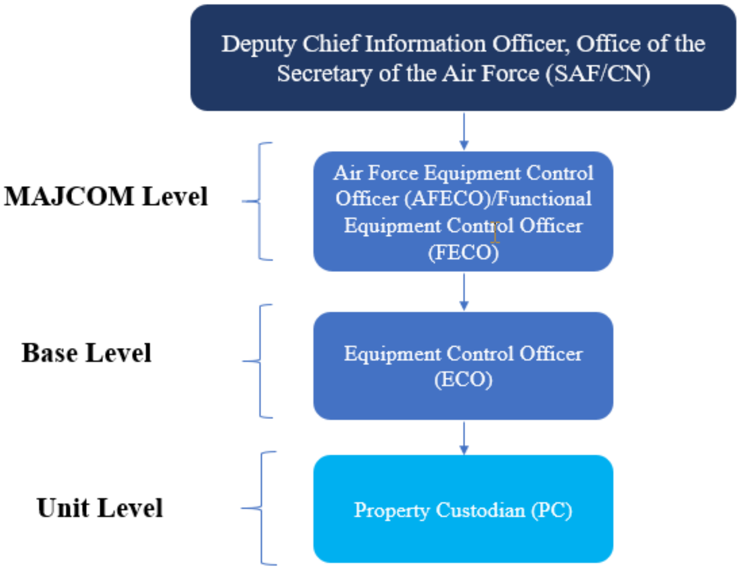
2.3. Roles and Responsibilities. Figure 2.1 and **Figure 2.2** represent an overview of those hardware asset management roles and responsibilities from the Air Force to the organizational level.

Figure 2.1. Property (Physical) Accountability Roles Overview.


Deputy Chief Information Officer, Office of the Secretary of the Air Force (SAF/CN)
Base Level
Host Installation /Wing Commander
Host /Tenant Accountable Property Officer (APO)
Equipment Control Officer (ECO)
Unit Level
Unit Accountable Property Officer (UAPO)
Property Custodian (PC)

Note: The APO role in DPAS is not the same as the Host/Tenant APO or UAPO level. The Host/Tenant APO and UAPO do not require DPAS access or training.

Figure 2.2. Asset (Financial) Reporting Roles Overview.


Deputy Chief Information Officer, Office of the Secretary of the Air Force (SAF/CN)
MAJCOM Level
Air Force Equipment Control Officer (AFECO)/Functional Equipment Control Officer (FECO)
Base Level
Equipment Control Officer (ECO)
Unit Level
Property Custodian (PC)

2.3.1. Air Force Equipment Control Officer (AFECO).

2.3.1.1. The Cyberspace Capabilities Center (CCC) within Air Combat Command (ACC) serves as the AFECO for all Air Force IT hardware assets within DPAS in accordance with **Attachment 2**.

2.3.1.2. Provides guidance and support to MAJCOMs, FOAs, and DRUs in managing IT hardware assets.

2.3.1.3. Reviews, evaluates, and interprets issues and problems as the ITAM subject matter expert and makes recommendations on ITAM policy changes to SAF/CN.

2.3.1.4. Coordinates with SAF/CN to propose changes, upgrades, and/or modifications to DPAS in accordance with **Attachment 2**.

2.3.1.5. Tracks the appointment of FECOs.

2.3.1.6. Maintains a list of designated FECOs and Equipment Control Officers (ECOs).

2.3.1.7. Manages the implementation of DOD and Air Force policy on Serialized Item Management (SIM) in accordance with DODI 8320.04, *Item Unique Identification (IUID) Standards for Tangible Personal Property*, for all IT hardware assets managed in DPAS in accordance with **Attachment 2** as applicable. **(T-0)**.

2.3.1.8. Maintains a list of Host/Tenant APOs appointments and notifies SAF/CN of required appointments.

2.3.1.9. Has authority to freeze a primary asset account for failure to comply with requirements described in this policy.

2.3.1.10. Monitors excess IT asset inventories in DPAS, monitors spare levels, and provides guidance on utilizing excess IT hardware assets.

2.3.1.11. Ensures compliance with this AFGM.

2.3.1.12. Resolves compliance issues that cannot be resolved at the Host/Tenant APO level.

2.3.1.13. Provides reports to MAJCOM A6s or MAJCOM inspection teams when requested.

2.3.1.14. Serves as DPAS Catalog Manager to standardize the catalog and create new catalog records for each unique stock number, manufacturer name, model number, and manufacturer Commercial and Government Entity code (CAGE) code combination.

2.3.2. Air Force IT Business Analytics Officer (IT-BAO).

2.3.2.1. Serves as the primary office for data analysis of all Air Force IT hardware and software asset spend and utilization.

2.3.2.2. Defines, develops, and tracks standard IT category performance metrics to support IT asset hardware and software life cycle processes.

2.3.2.3. Benchmarks, tracks, and reports performance-based metrics to support IT Category Asset Management efforts.

2.3.2.4. Provides IT spend and asset utilization reports to SAF/CN, lead commands, and others, as requested.

2.3.3. Functional Equipment Control Officer (FECO).

2.3.3.1. Serves as the liaison between the AFECO and ECO.

2.3.3.2. Will not serve as FECO and ECO in the same command according to DOD FMR 7000.14-R, Volume 3, Chapter 8, *Standards for Recording and Reviewing Commitments and Obligations and* AFI 65-201, *Managers' Internal Control Program Procedures*. **(T-0)**.

2.3.3.3. Completes additional training as directed by the AFECO.

2.3.4. Host Installation Commander, Wing Commander (or equivalent).

2.3.4.1. Must appoint the Host APO and maintains appointment letters on file. **(T-1)**.

2.3.4.2. Must appoint Tenant APOs in the Host Tenant Support Agreement (HTSA), as necessary. **(T-1)**.

2.3.5. Host/Tenant Accountable Property Officer (APO).

2.3.5.1. Must be appointed by the host installation commander, Wing Commander (or equivalent). **(T-1)**.

2.3.5.2. Will serve as the accountable officer for all IT hardware on their installation. **(T-1)**.

2.3.5.3. Must appoint at least one primary and one alternate ECO, document acknowledgement of duties with handwritten or digital signatures, and provide a copy to the AFECO/FECO. **(T-1)**.

2.3.5.4. Will ensure the DPAS inventory provides accountability of all IT hardware assets in accordance with this manual. **(T-1)**.

2.3.5.5. Must be accountable for all IT assets on their installation, unless otherwise delegated in an HTSA. **(T-1)**.

2.3.5.6. Will ensure assets are accounted for throughout their lifecycle. **(T-1)**.

2.3.5.7. Will ensure assets are stored according to environmental specifications of a manufacturer. **(T-1)**.

2.3.6. Equipment Control Officer (ECO).

2.3.6.1. Must be appointed as primary or alternate by the Host/Tenant APO. **(T-1)**.

2.3.6.1.1. Will be, at a minimum, the rank of E-5 or GS-7. There is not a rank/grade minimum requirement for an alternate ECO. **(T-1)**.

2.3.6.1.2. If contractor employees are assigned to perform ECO duties under the terms of a contract, the Air Force will retain responsibility for obligating funds and receiving assets as they are inherently governmental functions according to Federal Acquisition Regulation (FAR) Subpart 7.5, *Inherently Governmental Functions.* **(T-0)**.

2.3.6.1.3. Must not be appointed as a Resource Advisor (RA) within the same unit in which they are performing duties as ECO, nor will they be the Government Purchase Card (GPC) holder for IT assets. **(T-1)**.

2.3.6.2. Will process the receipt, transfer and disposal of all IT assets and complete necessary documentation to establish custodial responsibility. **(T-1)**.

2.3.6.2.1. Will assist property custodians (PC) in determining the ownership, reassignment or disposition of all Found-on-Base (FOB) IT assets. **(T-1)**.

2.3.6.2.2. Will direct PCs to conduct inventories in accordance with **Attachment 3**. **(T-1)**.

2.3.6.2.3. Will provide PCs with asset labels. **(T-1)**.

2.3.6.3. Will monitor AFECO collaboration sites for additional guidance and support. **(T-1)**.

2.3.6.4. Will complete additional training as directed by the AFECO/FECO. **(T-1)**.

2.3.6.5. Will provide PCs with training on requirements and standardized procedures. **(T-1)**.

2.3.6.6. Will provide inventory assistance in accordance with **Attachment 3**. **(T-1)**.

2.3.6.7. Will ensure on hand serviceable spares for desktops and laptops only do not exceed 5% of the total inventory at their assigned unit. If 5% does not equal one asset, the spare level will be one asset. **(T-1)**.

2.3.7. Unit APO (UAPO). Organization commanders (or equivalent) shall serve as UAPO and are responsible for providing guidance and procedures to ensure adequate protection and oversight is afforded to IT assets under their control.

2.3.7.1. Will appoint at least one primary and one alternate PC per account in accordance with DODI 5000.64, *Accountability and Management of DOD Equipment and Other Accountable Property,* section 3.2, paragraph f, and document acknowledgement of duties with handwritten or digital signatures and provide a copy to the ECO. **(T-0)**.

2.3.7.2. Must be responsible for the accountability of all IT hardware and software assets assigned to their unit. **(T-1)**.

2.3.7.3. Will ensure assets are inventoried according to **Attachment 3**. **(T-1)**.

2.3.7.4. Will ensure PC perform out-of-cycle inventories as directed. **(T-1)**.

2.3.7.5. Must direct PC to complete a gain-loss inventory no later than 30 calendar days prior to out processing for losing organization commander or custodian changeover. **(T-1)**.

2.3.7.6. Will monitor the acquisition, storage, utilization, and disposition of property within his or her assigned accountable area. Identify underutilized, impaired, or obsolete property and take appropriate actions to increase utilization or ensure disposition. **(T-0)**.

2.3.7.7. Will develop physical inventory plans and procedures, schedule physical inventories, and assist in their completion in accordance to **Attachment 3**. **(T-0)**.

2.3.7.8. Will ensure on hand serviceable spares for desktops and laptops only do not exceed 5% of the total inventory at their assigned unit. If 5% does not equal one asset, the spare level will be one asset. **(T-1)**.

2.3.7.9. Will ensure PCs complete required training. **(T-2)**.

2.3.8. Property Custodian (PC).

2.3.8.1. UAPO must appoint primary or alternate PC in writing. **(T-1)**.

2.3.8.2. Contractors may serve as PC, if allowable under the contract terms and conditions and approved by the organization commander.

2.3.8.2.1. PCs shall be accountable for all assigned IT hardware assets within their respective custodian accounts. **(T-1)**.

2.3.8.3. Will perform, at a minimum, an annual inventory of all assets under their purview, as prescribed in DODI 5000.64. **(T-0)**.

2.3.8.4. Will ensure all accountable assets have labels generated with IUID or equivalent, including part number and serial number prior to being placed in service. **(T-1)**.

2.3.8.5. Will notify ECO of all shipments (incoming and outgoing), transfers, donations, or turn-ins of excess assets. **(T-1)**.

2.3.8.6. Will provide appropriate documentation to the applicable ECO to clear the account of equipment that was shipped to another base/location, transferred to another account, or turned in to the Defense Logistics Agency Disposition Services (DLADS). **(T-1)**.

2.3.8.7. Must be approved to out-process by the UAPO and ECO. **(T-1)**.

2.3.8.8. Upon discovery of lost, damaged, or destroyed assets:

2.3.8.8.1. PC must notify the ECO and organization commander or equivalent. **(T-1)**.

2.3.8.8.2. PC must report the loss of any IT hardware asset with persistent storage to the Information System Security Office (ISSO) or wing information Assurance (IA), Information Protection (IP), or PII according to requirements outlined in AFI 17-130, Air Force I 16-1404 to AFI 16-1404, *Air Force Information Security Program*, and any local procedures. **(T-1)**.

2.3.8.9. Must ensure hard drives are removed from assets prior to turn-in to DLADS and must contact ISSO or wing IA to obtain sanitization procedures for hard drives. **(T-1)**.

2.4. Accountability Rules of IT Hardware Assets.

2.4.1. Accountability Technique Determination. Accountability and responsibility of IT hardware assets resides with the wing and unit commanders, who serve as the Host/Tenant APO or the UAPO, respectively. Physical and financial accountability takes place throughout the lifecycle of the asset. In accordance with DODI 5000.64, accountability of Air Force IT hardware assets is determined as follows:

2.4.1.1. Must be established upon receipt, delivery, or acceptance. **(T-0)**.

2.4.1.2. Is enabled by serialized numbering for identification, tracking, and management in accordance with DODI 8320.04. **(T-0)**.

2.4.1.3. Is established and maintained using Automated Identification Technology (AIT), to include the use of barcode printers, hand-held and tethered scanners, radio frequency identification, tablets, and common access card readers. AIT will be further supported by the use of electronic forms, attachments, or other soft copies of documentation where practicable.

2.4.1.3.1. Must use AIT to assist in property accountability unless it is unavailable or demonstrably proven through cost benefit or other analysis that implementation would not be practical. **(T-0)**.

2.4.1.3.2. Decisions of "not practicable" must be documented by a memorandum of record and reevaluated and reaffirmed every 2 years. The memorandum of record must be signed by PC, provided to UAPO, and be available upon request (e.g., audit). **(T-0)**.

2.4.1.4. Is maintained throughout the property's useful life and through disposal regardless of the property's status within the property life cycle (e.g., excess, obsolete or unserviceable, surplus) or its physical location (e.g., loading platform, in-transit, in theater). **(T-0)**.

2.4.2. Controlled Inventory IT Hardware Assets.

2.4.2.1. Controlled Inventory IT assets are any IT hardware with persistent storage (e.g., laptop, desktop, server, tablet, smartphone, external hard drive, and thumb drive). Persistent storage does not include device firmware.

2.4.2.2. Controlled Inventory assets must be accounted for in DPAS in accordance with **Attachment 2** due to their capability to process and/or transmit personally identifiable information or another sensitive agency information according to DODI 5000.64. **(T-0)**. Physical accountability of these items is required in support of IT configuration management and cybersecurity requirements. Physical accountability supports the goal of automating the association of IT assets with network configuration management items and to enhance overall cyberspace situational awareness of physical assets. **(T-1)**.

2.4.2.3. ECOs will report the loss of any IT asset with persistent storage and/or PII to the ISSO, Wing Cybersecurity Office (WCO) or Information Protection (IP) office, according to requirements outlined in AFI 17-130, and AFI 16-1404, and any local procedures. **(T-1)**.

2.4.3. Accountable Property Records (APR).

2.4.3.1. Accountable property records will be established in DPAS in accordance with **Attachment 2** for:

2.4.3.1.1. All government property purchased or otherwise obtained having a unit acquisition cost of $5,000 or more. **(T-0)**.

2.4.3.1.2. Assets obtained via a capital lease, as defined in DODI 5000.64. **(T-0)**.

2.4.3.1.3. Classified assets as defined in DODI 5000.64. **(T-0)**.

2.4.3.1.4. Assets qualified as a sensitive asset as defined in DODI 5000.64. **(T-0)**.

2.4.3.1.5. Assets categorized as Government Furnished Property (GFP) as defined in DODI 5000.64. **(T-0)**.

2.4.3.2. Any IT asset/item meeting the criteria for this category will be managed using DPAS in accordance with **Attachment 2**. **(T-1)**.

2.4.3.3. PC will ensure accountable property records are be kept current and reflect the current status, location, financial information, and condition of the asset until authorized disposition of the property occurs. The property records must provide a comprehensive log of suitable key supporting documents (KSDs) for audit. They will also be the authoritative source for use in validating the existence of transactions and completeness of an asset. **(T-1)**.

2.4.4. Accountability Record (AR) Process.

2.4.4.1. An IT asset/item will be accounted for using the AR process if any of the following criteria applies:

2.4.4.1.1. The asset/item has a unit acquisition cost of less than $5,000 but is controlled or managed at the asset/item level in accordance with DODI 4151.19, *Serialized Item Management (SIM) for Life-Cycle Management of Materiel*. **(T-0)**.

2.4.4.1.2. The asset/item has the capability to store personally identifiable information (PII). **(T-0)**.

2.4.4.1.3. The asset/item was obtained via an operating lease, as defined in DODI 5000.64. **(T-0)**.

2.4.4.1.4. Core network and data management infrastructure with unit cost of less than $5,000. Core infrastructure are devices that enable management of network services, e.g., servers, routers, switches, and firewalls. **(T-1).**

2.4.4.2. Any IT asset/item meeting the criteria for this category will be tracked in DPAS in accordance with **Attachment 2**. **(T-0)**.

2.4.5. Accounting for Information Technology Assets that do not meet the criteria for the APR or AR processes.

2.4.5.1. For an IT asset/item that does not meet any of the criteria described in **paragraph 2.4.3.** or **2.4.4.**, the Air Force does not require accountability and tracking, but does not preclude an organization from doing so.

2.4.5.2. UAPOs may direct PCs to account for these assets with locally developed procedures.

2.4.5.3. In accordance with DODI 5000.64, paragraph 4.5 (j), printers obtained via an operating lease that do not follow the APR/AR process and are not required to be tracked in DPAS should be accounted for in local systems.

2.4.5.4. IT Assets that are peripherals and other IT hardware lacking both persistent storage and IP network capabilities (e.g., mouse, keyboard, monitor, non-network displays, non-network capable Keyboard Video Mouse (KVM) switch, Voice Over Internet Protocol (VOIP) telephones, non-network capable fax machine, and non-network capable printer). Additional IT assets include IT hardware providing Wireless Personal Area Network (WPAN) capabilities without IP network capabilities (e.g., wireless mouse and Bluetooth keyboard). These assets are not required to be tracked in DPAS but may be accounted for on local systems at the request of the UAPO.

2.4.6. IT Hardware Accountability in DPAS.

2.4.6.1. Any asset recorded, tracked, and managed in the DPAS in accordance with **Attachment 2** must:

2.4.6.1.1. Adhere to the requirements described in DODI 5000.64, Section 4. **(T-0)**.

2.4.6.1.2. Be inventoried at least annually. **(T-0)**.

2.4.6.1.3. Only be updated in DPAS in accordance with **Attachment 2** with the appropriate documentation, such as disposal or transfer documentation, Accountable Property Inventory Adjustment Worksheet (APIAW), DD Form 200, *Financial Liability Investigation of Property Loss*, etc.

2.4.7. IT Components of a Weapon System or other Similar Capability. IT assets that are components of a Weapon System or other similar capability will be managed by this policy if both of the following apply:

2.4.7.1. The weapon system is not being managed in another APSR in accordance with **Attachment 2**, per AFI 23-111, *Management of Government Property in Possession of the Air Force*, and AFI 21-103, *Equipment Inventory, Status and Utilization Reporting.* **(T-1)**.

2.4.7.2. The IT components meet the requirements of **paragraph 2.4.3.** or **paragraph 2.4.4**. of this manual. **(T-1)**.

2.5. Procurement of IT Hardware Assets.

2.5.1. Approved procurement options. All Air Force IT hardware that meets APR and AR criteria must be procured using applicable Air Force IT Commodity Council (ITCC) enterprise buying programs via AFWay at https://www.AFway.Air Force.mil, or the GSA 2GIT contract vehicle when applicable. The following mandatory ITCC Blanket Purchase Agreements (BPAs) are available: Client Computing Solutions Quantum Enterprise Buy (CCS QEB), and Digital Printing & Imaging (DPI). The CCS QEB and DPI purchase sources are mandatory and take precedence over the GSA 2GIT contract, unless waived by the MAJCOM/A6 or equivalent. All print devices should be procured using guidance in **paragraph 2.5.3**.

Note: Effective 28 February 2019, all CONUS unclassified wireless devices and services transitioned to the "Navy Spiral 3 IDIQ contract in accordance with the SAF/CN policy. The Air Force will utilize a phased approach to transition to the Navy contracts. Air Force users can access the Navy Strategic Sourcing Site at: https://my.navsup.navy.mil/webcenter/portal/nss.

Non-NAVSUP users must register their CAC prior to access; register your PKI certificate in the NAVSUP Master Directory at: https://www.navsup.navy.mil/registration

2.5.1.1. All requests for servers must comply with current National Defense Authorization Act (NDAA). **(T-0)**. A DOD unique identifying number must accompany the acquisition. **(T-0)**.

2.5.1.2. Use the annual USAF Budget Guidance to maximize planning based on IT purchases related to program requirements and minimize reliance on year-end fall-out funds.

2.5.1.3. MAJCOM/A6s (or equivalents) shall approve a QEB or DPI waiver, however MAJCOMs and Program Offices must use either approved vendors from ITCC, or the GSA 2GIT contract vehicle to meet their mission requirements. **(T-1)**.

2.5.1.4. All Air Force IT hardware not available through ITCC BPAs are mandated to use the GSA 2GIT contract vehicle, when applicable. GSA 2GIT contracts provide access to vendors who can provide delivery of products, services and solutions that adhere to the Air Force Enterprise Architecture. **(T-1)**.

2.5.1.5. All Air Force IT procurements must use the Cyberspace Infrastructure Planning System (CIPS) for all IT requirements, regardless of dollar value to mitigate risk of infiltration of the supply chain by nation states.

2.5.1.6. Ensure products/solutions being requested are on the approved products list, are compatible with network architectures, are purchased from the original manufacturer or an authorized reseller and the technologies are not developed or hosted in sanctioned countries.

2.5.2. Procurement Process.

2.5.2.1. ECOs will ensure they provide complete information for shipping labels for ordered equipment. Obtain confirmation that procurement officials specify, as a contractual requirement, that "Ship To" and "Mark For" information is detailed on the shipping labels. This will alleviate problems with the receipt and acceptance processing of new hardware assets. **(T-1)**.

2.5.2.2. "Mark For" information will contain the recipient's name and unit, and may contain Contract Number, Purchase Order Number, Address, Phone Number, E-mail Address, Resource Manager Name, and UAPO (when applicable). **(T-1)**.

2.5.2.3. "Ship To" information will contain the complete delivery address. **(T-1)**. Assets shall be shipped to Central Receiving at the ECO's location and must include the recipient's name. **(T-1)**. This will correspond to the DOD Activity Address Code (DODAAC) and the Automated Civil Engineer System-Real Property ((ACES-RP) system of record for real property. **(T-1)**.

2.5.2.3.1. Central receiving facilities and warehouses must meet manufacturer operating and storage environment specifications, standard facility requirements and Department of the Air Force safety standards to protect assets from physical damage and inclement weather.

2.5.2.4. All Accountable IT hardware assets must be added to DPAS in accordance with **Attachment 2**. ECOs must ensure the correct MAJCOM and AUIC code is entered into DPAS for all asset(s) in their Primary Asset Account. The MAJCOM code must correctly identify the owning command, which may differ from the host base's command. If an asset is not loaded in the DPAS Catalog, the ECO must submit a catalog update request through the AFECO. **(T-1)**.

2.5.2.5. End user devices might be refreshed at recommended refresh schedule based on industry standards outlined in **Table 2.1**.

Table 2.1. End User Device Refresh Rate

Device Type	**Recommended**
Desktop	4 years
Laptop/Notebooks	4 years
Tablet	4 years
Mobile Devices	2 years
Printer	5 years
Radio	10 years

2.5.3. Managed Print Services (MPS). The goal of MPS is to reduce overlap in procuring print devices and the number of print devices throughout the enterprise by managing contract spending through a balance of government-wide, agency-wide, and local contracts.

2.5.3.1. MAJCOMs will comply with Managed Print Services (MPS) in order to streamline contract procurement, print anywhere, secure printing, increase document automation, and reduce assets aligned with End User Device Portfolio and Category Management catalog of services. **(T-1)**.

2.5.3.2. New MPS contracts must be procured through either Defense Logistics Agency (DLA) Equipment Management Solutions or General Services Agency (GSA) Schedule 36, SIN 51-500. Contact local contracting office for guidelines to executing an MPS contract/obtaining print services. **(T-1)**.

2.5.3.3. MAJCOMs will maintain a minimum of a 1:12 printer to user's ratio for each network enclave. Facilities/enclaves with fewer than 12 users will be limited to a single printer. **(T-2)**.

2.5.3.4. IT BAO will measure contract spend, asset inventory, and provide metrics to SAF/CN, the Air Force IT Category Manager, and each MAJCOM A6. IT BAO will be the point of contact (POC) for questions concerning MPS. **(T-1)**.

2.6. Receipt and Acceptance of IT Hardware.

2.6.1. Receipt and Acceptance of IT H Assets in DPAS. IT asset accountability must be established by formal receipt and acceptance in DPAS according to DODI 5000.64. Air Force IT asset accountability will be conducted in a timely manner using the following procedures. **(T-0)**.

2.6.1.1. The ECO or supporting personnel will receive and secure assets until proper accountability in DPAS is established in accordance with **Attachment 2**. **(T-1)**.

2.6.1.1.1. The ECO or supporting personnel will enter newly received IT assets into DPAS. **(T-1)**.

2.6.1.1.2. If other than the ECO receives IT hardware assets, the individual must inform the ECO of the delivery of the asset(s) and secure the asset(s) in a controlled access space until the asset(s) can be delivered, picked up, or otherwise addressed by the ECO. **(T-1)**. The asset(s) key supporting documents (KSD) will be provided for upload into DPAS within 7 calendar days of receipt and acceptance. **(T-1)**. Capital assets must be recorded by the end of the month or within 7 calendar days, whichever is sooner. **(T-1)**.

2.6.1.1.3. If an asset cannot be found in the current DPAS catalog, the ECO will request new catalog updates through the AFECO SharePoint site. **(T-1)**.

2.6.1.1.4. Prior ECO approval is required when delivering assets to geographically separated units (GSUs) and/or deviating from the standard ECO asset(s) delivery process.

2.6.1.2. For equipment not immediately installed, the ECO or supporting personnel will load assets into DPAS using the appropriate IT asset condition code in accordance to the **Attachment 2**. **(T-1)**.

2.6.1.3. Ensure unique asset identification is established for each item according to DODI 8320.04. **(T-0)**.

2.6.1.3.1. When the device is too small, user-generated labels that include Commercial and Government Entity (CAGE) code, part number, and serial number will be used. **(T-1)**.

2.6.1.3.2. Serialized labels will either be affixed to the asset by the manufacturer or will be applied by the ECO. **(T-1)**.

2.6.1.3.3. If the labels placed onto the asset by the manufacturer do not match manufacturer CAGE, part# and serial # or if the label placed by the manufacturer does not match the data entered in DPAS in accordance with **Attachment 3** for the asset, then the ECO must place a label with the correct manufacturer CAGE, part# and serial matching the data in DPAS must be placed onto the item. **(T-1)**.

2.6.2. Project Management Office (PMO).

2.6.2.1. PMOs will coordinate with ECOs and PCs to ensure assets being installed or brought to an installation are loaded into DPAS.

2.6.3. DPAS Structure.

2.6.3.1. APOs along with ECOs, will determine the best way to align their IT asset accounts within DPAS by using one of two below Air Force approved DPAS account structures. **(T-1)**.

Structure 1: Use AUIC to identify the location, multiple UICs to identify units, and multiple Custodians to identify unit accounts

Example:
AUIC: Scott AFB
UIC: Communications Squadron
Custodian: Cable Maintenance work center
    Custodian: Radio Maintenance work center
    UIC: Security Forces Squadron
        Custodian: Alert Forces work center
Custodian: Flightline Security work center

Structure 2: Use AUIC to identify the location, AUIC to identify the location, and custodians to identify units and unit accounts

Example:
AUIC: Scott AFB
UIC: Scott AFB
Custodian: Communications Squadron Cable Maintenance work center
        Custodian: Communications Squadron Radio Maintenance work center

2.7. Sustainment of IT Hardware Assets.

2.7.1. Inventory.

2.7.1.1. Purpose**.** The purpose of an inventory is to ensure all assets reported on the general ledger and the financial statement exist and can be readily located. Any assets in the possession of the Air Force must be accounted for in DPAS in accordance with applicable property and financial management policies and as prescribed in DODI 5000.76. **(T-0)**.

2.7.1.2. Frequency.

2.7.1.2.1. Assets meeting the accountability criteria for Accountable Property Record (APR) and the Accountability Record (AR) stated in **paragraph 2.4.3**. and **2.4.4.** will be inventoried annually. **(T-0)**.

2.7.1.2.2. Assets in **paragraph 2.4.5**. that do not meet the accountability criteria for APR or AR process have no prescribed inventory frequency.

2.7.1.2.3. IT asset inventory methods may include but are not limited to: Automatic Identification Technologies (AIT), network software inventory tools, e.g., SCORE, Tanium ®, FITARA, etc; and routine maintenance and or service events.

2.7.1.3. Inventory Requirements. Specific guidance on the minimum requirements applicable to all units in the Air Force for the inventory of IT assets can be found in **Attachment 3**.

2.7.2. Reports of Survey (ROS).

2.7.2.1. The APO shall initiate an investigation into certain lost, damaged, or stolen property that meets the requirement prescribed in DOD FMR 7000.14-R, Vol 12, Chap 7, *Financial Liability for Government Property Lost, Damaged, Destroyed, or Stolen*. **(T-0)**.

2.7.2.2. The ECO responsible for the report of survey must document the investigation on a DD Form 200 unless it is one of the exceptions found in DOD 7000.14-R, Vol 12, Chap 7. **(T-0)**.

2.7.2.3. The ECO should contact installation ROS Manager for additional information.

2.7.2.4. Managing Capital Assets. *The Chief Financial Officers (CFO) Act of 1990*, 31 U.S.C. §§901-903, specifies financial reporting and acquisition cost depreciation is required for equipment meeting the capitalization threshold as stated in DOD FMR 7000.14-R, Volume 4, Chapter 25, *General Equipment*. Acquisition cost will include all costs incurred to bring the asset to a form and location suitable for its intended use (e.g., amounts paid to vendors, transportation to point of initial use, handling and storage costs, interest costs paid, and direct and indirect production costs). **(T-0)**. *Note: Acquisition cost is used to determine depreciation.*

2.7.2.5. Contractor Guidance. Establish the extent of contractor liability in the provisions of the applicable contract's government property clause according to AFI 23-111.

2.8. Disposition of IT Hardware Assets.

2.8.1. Transfers. When transferring equipment, all documentation applicable to the lifecycle of that asset (e.g., acquisition documentation, invoices, etc.) must be transferred along with that asset to the gaining organization, whether internal or external to the Air Force. **(T-1)**.

2.8.1.1. The transfer of non-excess IT assets occurs when a function (e.g., base realignment and closure), and the IT assets acquired to support that function, is transferred to another DOD component or Federal agency.

2.8.1.1.1. The PC of the losing organization will provide electronic documentation to the losing ECO outlining the transfer. This documentation will be electronically signed by the losing organization commander documenting the transfer of the function and equipment. **(T-1)**.

2.8.1.1.2. The PC and designated official from the shipping activity (Traffic Management Office or commercial carrier) must sign and date a DD Form 1149, *Requisition and Invoice/Shipping*

Document. For local transfers where no shipping activity is involved, the gaining and losing PC must sign the DD Form 1149. **(T-1)**.

2.8.1.1.3. The losing activity ECO:

2.8.1.1.3.1. Accounts for the transferred hardware. The ECO will identify excess hardware created as a result of the transfer of a function. **(T-1)**.

2.8.1.1.3.2. Updates the asset status field in DPAS using the condition codes in **Attachment 2**.

2.8.1.1.3.3. Provides account records information to the gaining activity as required.

2.8.1.1.3.4. Reviews all contract obligations with the gaining and losing activities and contracting officials. Pay close attention to any contract termination clauses (applies when extra maintenance has been paid for by the losing organization). Use currently established DPAS guidance for the removal of items from an account.

2.8.1.1.4. The losing ECO and the gaining ECO or other accountable officer:

2.8.1.1.4.1. Identify and report maintenance contracts that supported transferred assets to contracting officials.

2.8.1.1.4.2. Assist contracting officials as required, in transferring contracts to the gaining activity.

2.8.1.1.4.3. Review hardware assets release dates. Give adequate notice to the vendor to preclude payment of extra costs.

2.8.1.1.4.4. Coordinate hardware assets release dates with other base functions, as required.

2.8.1.1.4.5. Ensure hard drive sanitization according to AFMAN 17-1301 Chapter 6, *Computer Security (COMPUSEC)*, and National Security Agency/Central Security Service Policy Manual 9-12, *NSA/CSS Storage Device Sanitization Manual*.

2.8.1.1.4.6. Provide the hardware system database records or custodian report to the PC. The PC will add all applicable records regarding the transfer to their applicable electronic records in DPAS. (T-1).

2.8.1.1.4.7. Properly inventory, package, warehouse, and secure equipment when storing hardware assets before transfer.

2.9. Excess IT Hardware Assets.

2.9.1. Disposition of Excess Hardware Assets.

2.9.1.1. An item is in excess when it is no longer required due to mission change, equipment upgrades, technology changes, obsolescence, etc. The item is also considered excess when the total quantity on hand exceeds the required quantity, as identified in the technical solution/requirements document, plus the number of authorized spares as identified in the

Acquisition Strategy, Lifecycle Master Plan, and Lifecycle Support Plan (AS/LCMP/LCSP). Reference AFI 63-101/20-101, *Integrated Lifecycle Management* for further information about the AS/LCMP/LCSP. According to AFI 23-111, accountable individuals are responsible for properly identifying, reporting, and determining correct disposition of unserviceable, reparable, or excess property**.**

2.9.1.2. The PC will not permanently retain serviceable excess asset items as mandated by SAF/CN guidance. Serviceable excess assets will have a condition code of "C" in DPAS and be redistributed to other units as needed. If assets cannot be redistributed, they will be condition coded as "K" and turned in to DLADS. For further information on DPAS Condition Codes, see **section A2.3.10**. **(T-1)**.

2.9.1.3. The PC will notify the ECO when hardware assets will become excess no later than 30 calendar days before the equipment goes off-line if possible. This allows completion of the screening cycle while the equipment is still in use, eliminating the need to store excess assets. If not possible, until receipt of final disposition instructions, the PC will store the equipment to prevent damage, deterioration, or unauthorized cannibalization. **(T-1)**.

2.9.1.4. When an organization receives a replacement IT asset for a technical refresh or replaces an unserviceable asset, the organization must turn in the asset being replaced and remove it from the APSR within 30 calendar days after receipt of the replacement asset. The owning PC will coordinate with the ECO, and the Information System Security Office (ISSO) or wing Information Assurance (IA), in order to process the disposal to DLADS. **(T-1)**.

2.9.1.5. Upon receipt of the replacement asset, the ECO will assign the asset being removed with condition code "K", "Ready for turn in," in the APSR. This condition code will remain on the asset until the PC turns the asset over to DLADS. Once the ECO receives the documentation certifying the asset has been turned in to DLADS, the ECO will remove the asset from the APSR. No further assets will be purchased by the unit until the assets being replaced have been removed from the APSR. **(T-1)**.

2.9.1.6. Dispose of and/or reuse classified media and systems according to the guidance in **paragraph 2.10.3.1**.

2.9.2. Transferring and Obtaining Excess IT Hardware Assets.

2.9.2.1. The ECO may direct hardware asset reutilization for new requirements or to replace equipment that does not meet minimum standards when allowed by the parent MAJCOM.

2.9.2.2. Excess hardware may be transferred from ECO to ECO in DPAS. For instructions on transferring assets or any other transactional DPAS guidance, refer to the Quick Reference Guides (QRG) located on the DPAS Support site: https://dpassupport.golearnportal.org/index.php.

2.10. IT Hardware Assets Disposal.

2.10.1. The host installation and its regional DLADS facility will formalize a MOA to document the processes and procedures for how the installation will interact with DLADS for the disposal of IT hardware assets in accordance with DODM 4160.21, Vol 2, *Defense Materiel Disposition: Property Disposal and Reclamation*. **(T-0)**.

2.10.2. Elements of the MOA may be incorporated into the HTSA.

2.10.3. Prior to disposal:

2.10.3.1. The asset must have met all IT hardware sanitization requirements in accordance with AFMAN 17-130 and NSA/CSS Policy Manual 9-12. **(T-0)**.

2.10.3.2. All applicable documentation related to the disposal process must be completed and signed. **(T-0)**.

2.10.3.3. The disposing organization must plan and budget for disposal costs, to include packing and handling materials. **(T-2)**.

2.10.4. DLADS is the primary DOD agent for disposal of all obsolete, or unserviceable military property and equipment. All Air Force IT hardware will be disposed of through the DLADS. **(T-0)**.

2.10.4.1. DLADS guidelines for the disposal of hardware assets can be found at https://www.dla.mil/DispositionServices/.

2.10.4.2. All media being disposed of or transferred to DLADS or another entity outside of the DOD will be sanitized and/or destroyed as applicable according to AFMAN 17-1301. **(T-0)**.

2.10.5. The PA and PC may turn in equipment to DLADS when necessary, e.g., disposal, turn-in, etc.

2.10.5.1. The PC must provide the PA with all necessary details and/or KSDs for the transaction within 3 business days. **(T-2)**.

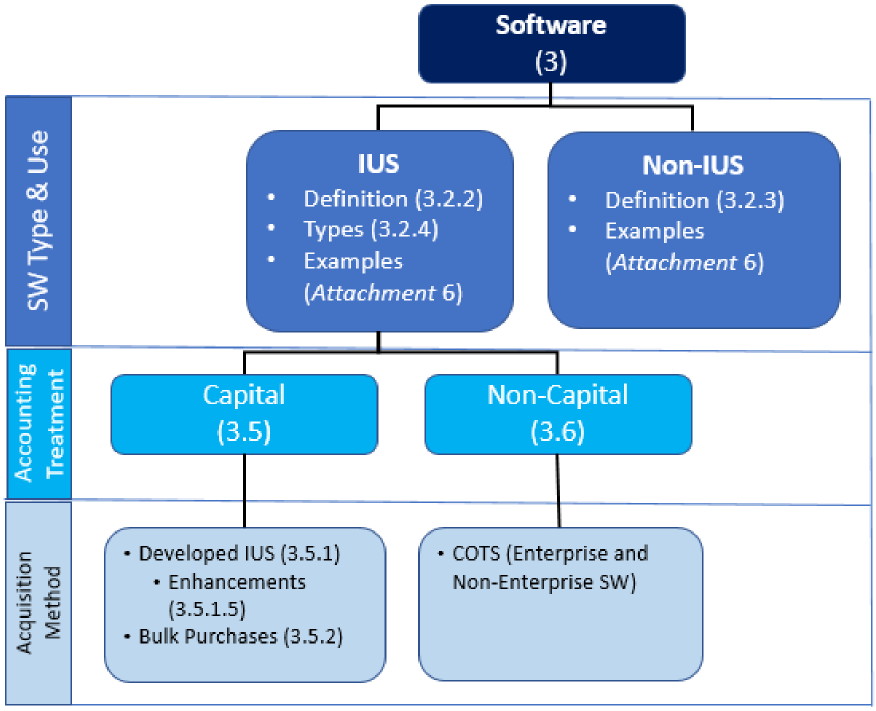
Chapter 3

SOFTWARE ASSET MANAGEMENT

3.1 Overview and Scope. This chapter provides guidance for physical and financial accountability and management of Department of the Air Force software, specifically IUS. It prescribes detailed processes and assigns roles and responsibilities to the key stakeholders that are responsible for procurement, management and disposal of software assets. Additionally, this chapter defines the difference between capital and non-capital IUS and prescribes detailed steps to account and financially report contractor-developed software and other COTS software that meet capitalization criteria.

This chapter excludes guidance for software that is not IUS (non-IUS). Examples of non-IUS software are embedded software, simulation software, utility programs, and software weapon systems and software as a service (SaaS). Embedded software such as software integrated or necessary to operate equipment (e.g., operating system, radar system, software internal to the weapons system) will be managed and accounted as part of the equipment in which it is installed. For a comprehensive list of IUS and non-IUS assets, refer to **Attachment 5**. Refer to **Figure 3.1** for software guidance organized by software type, accounting treatment, and acquisition method definitions and cross-references to governing para in this publication.

Figure 3.1. Software Guidance Breakdown.



3.2. Software Definition and Types.

3.2.1. Software Definition. Software includes the application and operating system programs, procedures, rules, and any associated documentation pertaining to the operation of a computer system or program.

3.2.2. IUS:

3.2.2.1. Is a stand-alone application, or the combined software components of an IT system that can consist of multiple applications, modules, or other software components integrated and used to fulfill an internal or operational need.

3.2.2.2. It is acquired or developed to meet internal or operational needs.

3.2.2.3. It is used to operate Department of the Air Force programs (e.g., financial and administrative software).

3.2.2.4. It is used to produce goods and provide services (e.g., maintenance work order management).

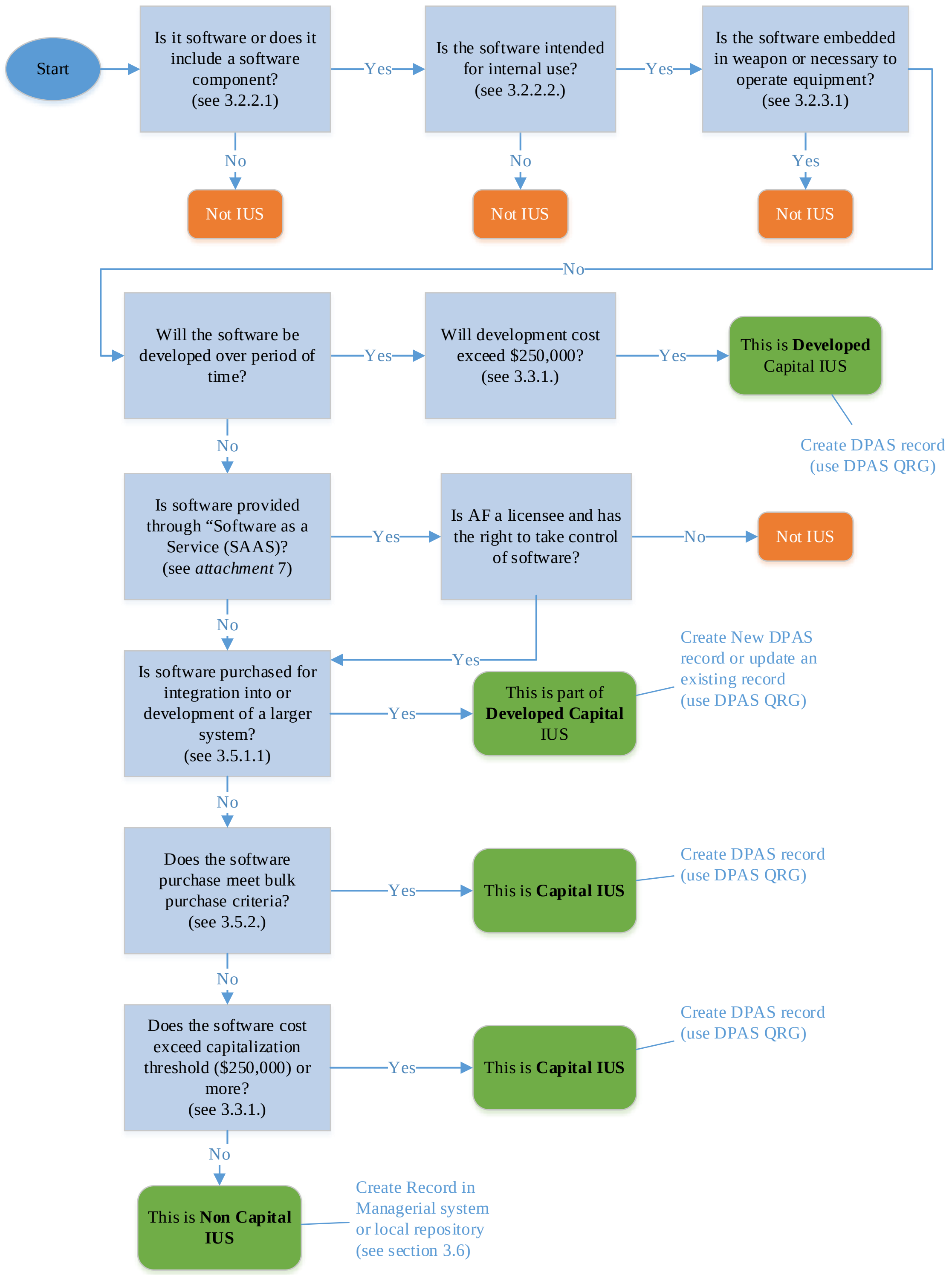
3.2.3. Non-IUS:

3.2.3.1. Software that is integrated into and necessary to operate equipment rather than perform an application (e.g., an operating system, radar systems, weapons system). To further clarify, software embedded within an equipment asset is not solely excluded upon classification as such. For software not to be considered IUS, it must be necessary to operate the equipment as intended. If the equipment could operate as intended upon removal of the software, the software is considered IUS. If the equipment cannot function as intended when separated from the software, then the software is not considered IUS and any costs for the software must be attributed to the equipment.

3.2.3.2. Software developed or acquired to sell to external parties.

3.2.3.3. To further determine whether an IT asset is IUS, please refer to **figure 3.2** below.

Figure 3.2. Internal Use Software Determination Flowchart.


Start
Is it software or does it include a software component? (see 3.2.2.1)
Yes
No
Not IUS
Is the software intended for internal use? (see 3.2.2.2.)
Yes
No
Not IUS
Is the software embedded in weapon or necessary to operate equipment? (see 3.2.3.1)
Yes
Not IUS
No
Will the software be developed over period of time?
Yes
Will development cost exceed $250,000? (see 3.3.1.)
Yes
This is **Developed** Capital IUS
Create DPAS record (use DPAS QRG)
No
Is software provided through "Software as a Service (SAAS)? (see *attachment* 7)
Yes
Is AF a licensee and has the right to take control of software?
No
Not IUS
Yes
No
Is software purchased for integration into or development of a larger system? (see 3.5.1.1)
Yes
This is part of **Developed Capital** IUS
Create New DPAS record or update an existing record (use DPAS QRG)
No
Does the software purchase meet bulk purchase criteria? (see 3.5.2.)
Yes
This is **Capital IUS**
Create DPAS record (use DPAS QRG)
No
Does the software cost exceed capitalization threshold ($250,000) or more? (see 3.3.1.)
Yes
This is **Capital IUS**
Create DPAS record (use DPAS QRG)
No
This is **Non Capital IUS**
Create Record in Managerial system or local repository (see section 3.6)

3.2.4. Types of Internal Use Software.

3.2.4.1. Commercial off-the-shelf (COTS) software:

3.2.4.1.1. COTS software is acquired from a vendor “as-is” and configured to be ready for use with minimal modifications.

3.2.4.1.2. Modified COTS software is pre-existing software that requires further development before it is ready for use for its intended function. Examples include but are not limited to creating interfaces with existing systems, configuring software to meet end-user requirements, creating new functionality, etc. Modified COTS are COTS purchased specifically for modification prior to being placed into service. If COTS software placed into service is going through modification, software enhancement rules apply as prescribed in **paragraph 3.5.1.5.**

3.2.4.2. Developed Software:

3.2.4.2.1. Contractor-developed software is software that the Air Force paid a contractor to design, program, install, and implement including new software and the modification of existing or purchased software.

3.2.4.2.2. Internally developed software is software developed and owned by a government agency. Typically, internally developed software is developed by the technical staff of the government agency (Air Force personnel) for which it is created.

3.2.4.3. For additional examples of IUS, please see Attachment 5.

3.3. Internal Use Software Financial Criteria.

3.3.1. IUS is recognized as capital if it meets the following criteria:

3.3.1.1. It is intended for use by the entity and not intended for sale in the normal course of business.

3.3.1.2. It has useful life of 2 or more years.

3.3.1.3. Full historical cost meets or exceeds $250,000.

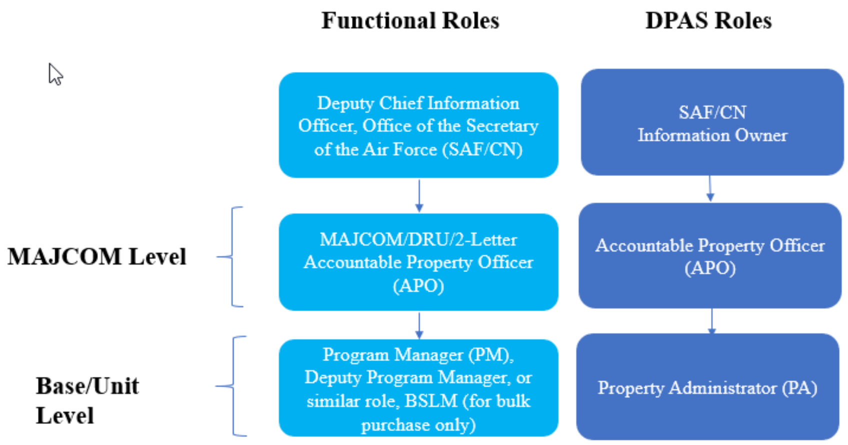
3.3.1.4. Additional capitalization criteria related to software licenses purchased in bulk and enhancements to the existing software is outlined in **paragraph 3.5.** of this guidance.

3.3.1.5. If IUS does not meet the above criteria, please follow processes prescribed in **paragraph 3.6.** of this guidance.

3.4. IUS Roles and Responsibilities.

3.4.1. Capital IUS Roles and Responsibilities. **Figure 3.3.** Provides an overview of roles and responsibilities for functional and DPAS role for management and accountability of capital IUS.

Figure 3.3. Capital Internal Use Software Roles.


Functional Roles
DPAS Roles
Deputy Chief Information Officer, Office of the Secretary of the Air Force (SAF/CN)
SAF/CN Information Owner
MAJCOM Level
MAJCOM/DRU/2-Letter Accountable Property Officer (APO)
Accountable Property Officer (APO)
Base/Unit Level
Program Manager (PM), Deputy Program Manager, or similar role, BSLM (for bulk purchase only)
Property Administrator (PA)

3.4.1.1. MAJCOM/DRU/2-Letter Accountable Property Officer (APO).

3.4.1.1.1. Serves as APO for all capital IUS assets owned by the organization.

3.4.1.1.2. Must ensure that all organization's capital IUS assets are accounted for in DPAS in accordance with DODI 5000.76. **(T-0)**.

3.4.1.1.3. Must ensure all accountable records for organization have the associated auditable information available for examination. **(T-1)**.

3.4.1.1.4. May delegate duties to additional APO to enable execution but the ultimate responsibility for execution will remain with the APO.

3.4.1.1.5. Must perform DPAS APO duties or delegate duties to alternative DPAS APO. **(T-1)**.

3.4.1.1.6. Must designate DPAS PA. **(T-1)**.

3.4.1.1.7. Must be a government civilian or military member. **(T-1)**.

3.4.1.2. Contracting Officer (CO).

3.4.1.2.1. Must write the contract, per requirements detailed in **Table 3.1** to itemize expenses requiring capitalization. **(T-1)**.

3.4.1.2.2. Must ensure contract line item number (CLIN) and sub-line numbering (SLIN) structure aligns with the lines of accounting assigned by requiring activities. **(T-1)**.

3.4.1.3. Contracting Officer Representative (COR) or equivalent.

3.4.1.3.1. Validates invoices for services performed that include developed IUS, for inclusion of valid CLIN or contract data requirements list (CDRL).

3.4.1.3.1. Notifies the vendor when CLIN or CDRL content is invalid or missing.

3.4.1.4. DPAS Information Owner (IO).

3.4.1.4.1. Serves as the Department of the Air Force level site owner for DPAS FF-CIOGE site.

3.4.1.4.2. Must be a government civilian or military member, currently assigned to SAF/CN. **(T-1)**.

3.4.1.4.3. Must approve or disapprove DPAS organization accounts. **(T-1)**.

3.4.1.4.4. Assists in resolving DPAS related issues for Air Force customers.

3.4.1.4.5. Must annually validate the APSR by utilizing DD Form 3041, DD Form 3041, *Accountable Property System of Record (APSR) Requirements Checklist for Internal Use Software (IUS).* **(T-1)**.

3.4.1.4.6. May delegate duties to additional IOs.

3.4.1.5. DPAS MAJCOM/DRU/2-letter Accountable Property Officer (APO).

3.4.1.5.1. Must serve as the key POC for all capital IUS assets owned by the organization.

3.4.1.5.2. Must ensure all capital IUS assets owned by the organization are being reported in DPAS. **(T-1)**.

3.4.1.5.3. Adds, updates, or deletes Unit Identification Codes (UIC) across the MAJCOM/DRU/2-letter, if necessary.

3.4.1.5.4. Must maintain the authoritative list of all capital IUS records owned by the organization and provide the list to SAF/CN or auditors as requested. **(T-1)**.

3.4.1.5.5. Must appoint in writing, DPAS Property Administrator (PA) and Base Software License Manager (BSLM) DPAS PA. **(T-1)**.

3.4.1.5.6. In coordination with DPAS PA and BSLM DPAS PA, must ensure that accountable records have associated auditable information available for examination. **(T-1)**.

3.4.1.5.7. Must perform, at a minimum, an annual inventory of all capital IUS assets owned by the organization, in compliance with DODI 5000.76. **(T-0)**.

3.4.1.5.8. Must take DPAS APO level trainings and obtain access to DPAS FF-CIOGE site. **(T-1)**.

3.4.1.5.9. Must be a government civilian or military member. **(T-1)**.

3.4.1.6. DPAS Property Administrator (PA).

3.4.1.6.1. This role is designated in coordination with IUS the owning organization’s APO that develops, deploys, and/or sustains the IUS throughout its lifecycle.

3.4.1.6.2. It can be performed by the PM, Deputy PM, Product Support Manager (PSM), functional system owner or any person designated by the APO that has the most visibility of capital IUS asset lifecycle.

3.4.1.6.3. Must serve as DPAS Catalog Manager (CM) and is directly responsible for establishing DPAS catalog items for capital IUS assets under their purview. **(T-1)**.

3.4.1.6.4. Works closely with the PM, COR, COR representative or COR equivalent to ensure contracts related to acquisition of developed IUS, included Contract Line Item Number (CLIN) structure detailed in **Table 3.1**. **(T-1)**.

3.4.1.6.5. Must collect and maintains all KSDs in support of IUS in Development, IUS placed in service, and major IUS enhancements, as prescribed in DOD FMR 700.14-R, Volume 4, Chapter 27, *Internal Use Software*, Section 270202. **(T-0)**.

3.4.1.6.6. Must update status of IUS in development in DPAS to indicate the completion of the IUS development phase and upload appropriate KSDs into DPAS record. **(T-1)**.

3.4.1.6.7. Must track and enter valid major IUS enhancement cost data, retain documentation related to IUS enhancement decisions, such as the justification for capitalizing the enhancement, a change of useful life, and the amount to be capitalized and upload supporting KSDs into capital IUS asset record established in DPAS. **(T-1)**.

3.4.1.6.8. Must notify DPAS APO of all IUS changes in capital IUS life-cycle events such as new record creation, completion of development activities, and initiation of major enhancements, transfer or disposal and provide supporting KSD(s) related to the life-cycle events. **(T-1)**.

3.4.1.6.9. Must take DPAS PA and CA level trainings and obtain access to DPAS FF-CIOGE site. **(T-1)**.

3.4.1.6.10. Can be a contractor, government civilian or military member.

3.4.1.7. Base Software License Manager (BSLM) DPAS PA.

3.4.1.7.1. This role applies to capital and non-capital IUS management.

3.4.1.7.2. Non-capital IUS management responsibilities for this role are outlined in **paragraph 3.4.1.6**.

3.4.1.7.3. Capital IUS responsibilities for this role include:

3.4.1.7.3.1. Must establish asset accountability record in DPAS for IUS that meets capitalization criteria as prescribed in **paragraph 3.2.1**. of this guidance, for any IUS that is not part of developed software.

3.4.1.7.3.2. Must monitor acquisition of COTS software bulk purchases in accordance with **paragraph 3.5.2**. of this guidance and establishes asset accountability record in DPAS if software meets COTS bulk purchase requirements. **(T-1)**.

3.4.1.7.3.3. Must maintain accountability records in DPAS and notify MAJCOM/DRU/2-letter DPAS APO if changes in the lifecycle of the asset record occur.

3.4.1.7.3.4. Must assist MAJCOM/DRU/2-letter DPAS APO with annual capital software asset inventory.

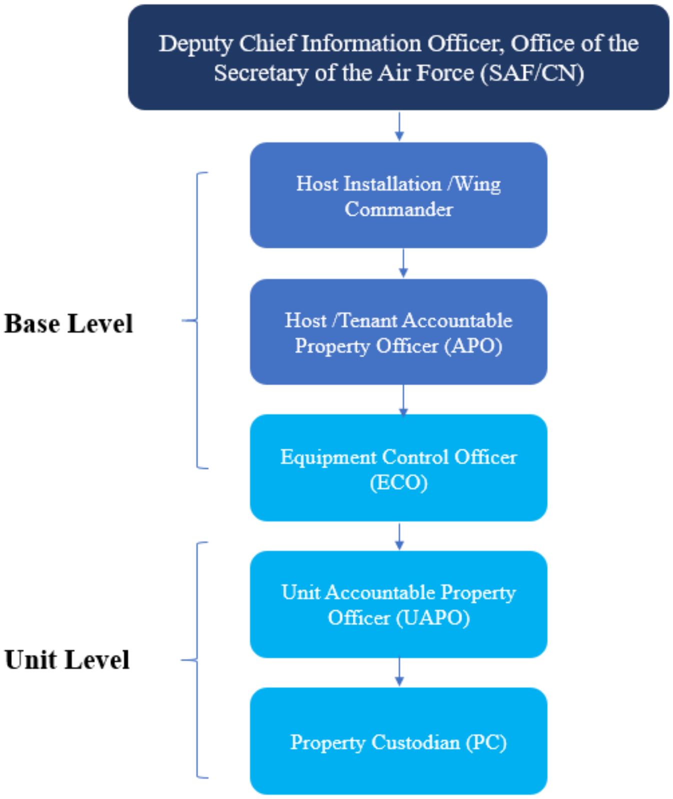
3.4.1.7.3.5. Might delegate duties to alternative DPAS PA as deemed appropriate.

3.4.1.7.3.6. Must take DPAS PA and CA level trainings and obtain access to DPAS FF-CIOGE site. **(T-1)**.

3.4.1.7.3.7. Can be a contractor, government civilian or military member.

3.4.2. Non-Capital IUS Roles and Responsibilities. Figure 3.4. provides an overview of roles and responsibilities for non-capital IUS management and accountability from the headquarters of the Air Force to the organizational level.

Figure 3.4. Non-Capital IUS Physical Accountability Roles.


Deputy Chief Information Officer, Office of the Secretary of the Air Force (SAF/CN)
Host Installation /Wing Commander
Base Level
Host /Tenant Accountable Property Officer (APO)
Equipment Control Officer (ECO)
Unit Accountable Property Officer (UAPO)
Unit Level
Property Custodian (PC)

3.4.2.1. Enterprise Software License Manager (ESLM).

3.4.2.1.1. Serves as the Department of the Air Force-wide software requirements manager for JELAs and other Air Force-wide licensing agreements, to include support of Combatant Commands for whom the Air Force is the Executive Agent.

3.4.2.1.2. Consolidates and analyzes software inventories to support JELA reporting requirements and ensures compliance with ELA requirements concerning appropriate availability, distribution and usage of the subject software.

3.4.2.1.3. Validates requirements approved by MAJCOM Software Benefits Administrators (SBAs) and submits price quote requests to the JELA vendor.

3.4.2.1.4. Provides approval of JELA contract modifications being processed by the applicable CO.

3.4.2.2. MAJCOM, DRU, FOA, or Equivalent.

3.4.2.2.1. Appoints in writing, a Software Benefits Administrator (SBA), documents acknowledgement of duties with handwritten or digital signatures in the appointment letter and retains a copy of the letter on file.

3.4.2.3. Software Benefits Administrator (SBA).

3.4.2.3.1. This is a MAJCOM, DRU, or 2-letter role.3.4.2.3.2. Ensures all COTS software products are purchased using approved DOD/Air Force Enterprise Licenses Agreements (ELAs), DOD ESI or approved DOD/Air Force contract vehicles. For SCI and ISR requirements, ensure IC ELAs and IC enterprise contract vehicles are used.

3.4.2.3.3. Acts as the liaison between BSLMs and the ESLM.

3.4.2.4. Host Installation Commander, Wing Commander (or equivalent).

3.4.2.4.1. Must Appoints the Host APO. **(T-1)**.

3.4.2.4.2. Appoints Tenant APOs in the HTSA, as necessary.

3.4.2.5. Host/Tenant Accountable Property Officer (APO).

.4.2.5.2. Will serve as the accountable officer for all software on their installation. **(T-1)**.

3.4.2.5.3. Will ensure the designated managerial system inventory record provides accountability of all software assets. **(T-2)**.

3.4.2.5.4. The host APO must be accountable for all software assets on their installation, unless otherwise delegated in an HTSA. **(T-2)**.

3.4.2.5.5. Will ensure assets are accounted for throughout their lifecycle. **(T-1)**.

3.4.2.5.6. Will designate primary and alternate BSLM (or equivalents) to manage the wing and/or base software license programs (to include applicable tenants) and informs their MAJCOM/A6 and service owner for Enterprise IT. **(T-2)**.

3.4.2.5.7. Must annually certify and document that software inventory was accomplished and the provisions of this AFGM guidance have been met. Provides a copy of the inventory to their MAJCOM/A6 and Service Owner for Enterprise IT. **(T-1)**.

3.4.2.6. Base Software License Managers (BSLM).

3.4.2.6.1. This role applies to capital and non-capital IUS management.

3.4.2.6.2. Capital IUS management responsibilities for this role are outlined in **paragraph 3.4.1.7**. of this guidance.

3.4.2.6.3. Will annually initiate and collect unit baseline inventories for all non-enterprise software for all organizations under BSLM purview and retain required inventory KSD) as prescribed by DODI 5000.76. **(T-0)**.

3.4.2.6.4. Will annually initiate and collect unit baseline inventories for all enterprise software that has been installed on stand-alone devices, as prescribed by DODI 5000.76. **(T-0)**.

3.4.2.6.5. Will assist ESLM in performing annual inventory of enterprise software licenses, reconcile them against contract information to maintain accountability of what has been purchased and to ensure adherence to legal use per contract terms. **(T-1)**.

3.4.2.6.6. Will provide annual inventories to higher headquarters as required or requested. **(T-1)**.

3.4.2.6.7. Will ensure unused or underutilized enterprise software licenses are identified, redistributed and reutilized. **(T-1)**.

3.4.2.6.8. Will provide software license training for USLMs, CSTs, helpdesk, and any other personnel responsible for managing licenses. **(T-1)**.

3.4.2.6.9. Will review enterprise software acquisition requests and works with SBA to verify that software is being procured using approved DOD/Air Force/IC ELAs, DOD ESI or approved DOD/Air Force/IC contract vehicles. **(T-1)**.

3.4.2.6.10. Will review software as a service (SaaS) subscription license agreements for accountability requirements and instruct USLM to establish accountability records if accountability requirements are met. **(T-1)**.

3.4.2.6.11. Will perform periodic compliance visits to base units and tenant organizations. **(T-1)**.

3.4.2.6.12. Will have the authority to deny software acquisition requests for failure of the organization to complete and submit annual software inventory. **(T-1)**.

3.4.2.7. Unit APO (UAPO).

3.4.2.7.1. This role is to be performed by the Commander (or their equivalent). The UAPO is responsible for providing guidance and procedures to ensure adequate protection and oversight is afforded to IT assets under their control. Examples of a “commander equivalent” include a Director of Staff, a civilian director of an organization, or a commandant of a school organization. See AFI 38-101, *Manpower and Organization*, for further guidance.

3.4.2.7.2. The UAPO will develop physical inventory plans and procedures, schedule physical inventories, and assist in their completion in accordance with DODI 5000.76. **(T-0)**.

3.4.2.7.3. Be responsible for the accountability of all IT software assets assigned to the unit. **(T-1)**.

3.4.2.7.4. Designates in writing, USLM or a similar role for unit software asset management. If USLM is not appointed by UAPO, USLMs duties will be performed by UAPO. **(T-1)**.

3.4.2.7.5. Must annually certify with via handwritten or digital signature indicating completion of baseline inventories for all non-enterprise software and all enterprise software that has been installed on stand-alone devices. **(T-1)**.

3.4.2.8. Unit Software License Manager (USLM).

3.4.2.8.1. Serves as the unit level focal point for managing the installation, coordination and removal of software on IT assets. Generates requests for, or provides validation of, software to be installed or removed from unit systems.

3.4.2.8.2. Manages all software licenses owned by the organization. **(T-1)**.

3.4.2.8.3. Coordinates all non-enterprise software acquisitions through the respective BSLM (or equivalents) prior to purchasing software. **(T-2)**.

3.4.2.8.4. Coordinates all enterprise software acquisitions through the respective BSLM and SBA (or equivalents) prior to purchasing software. **(T-2)**.

3.4.2.8.5. Establishes accountability of SaaS licenses per BSLM request, if they meet accountability requirements as prescribed in DODI 5000.76. **(T-0)**.

3.4.2.8.6. Establishes accountability of software licenses upon receipt of the invoice, maintains accountable records for the life of the asset and retain the records in accordance with DODI 5000.76 and National Archives and Records Administration's (NARA) standards, as described in NARA Directive 1571, *Archival Storage Standards* and DOD FMR 700.14-R, Volume 1, Chapter 9, *Financial Records Retention*. **(T-0)**.

3.4.2.8.7. Ensures unused or underutilized software licenses are identified to the BSLM (or equivalents) for redistribution, reutilization, or disposition to comply with Executive Order 13589, *Promoting Efficient Spending*. **(T-0)**.

3.4.2.8.8. Identifies locally owned software that does not have associated licenses, assemble proofs-of-purchase, and request replacement licenses from publishers, as needed. Develops plan of action to obtain compliance within 120 days. **(T-2)**.

3.4.2.8.9. Annually audits all computers and servers to ensure no illegal/unauthorized software is installed. **(T-2)**.

3.4.2.8.10. Performs annual and out-of-cycle inventories and submit to UAPO, BSLM, and ESLM as requested. **(T-1)**.

3.4.2.8.11. Conducts annual non-enterprise software inventory, utilizing auto-discovery tools when possible. **(T-1)**.

3.4.2.8.12. Conducts annual inventory for enterprise software that is installed on stand-alone devices. **(T-1)**.

3.4.2.8.13. Submits annual inventory to UAPO for approval and provides approved inventory to BSLM. **(T-1)**.

3.4.2.8.14. Performs out-of-cycle inventories as directed. **(T-2)**.

3.4.2.8.15. With the support of BSLM (or equivalents), ensures applicable training is conducted for users in support of unique software purchased or developed by organizations.

3.4.2.8.16. Identifies enterprise software license requirements and any management training requirements not covered in existing courses to the BSLM (or equivalents) for annual consolidation.

3.4.2.8.17. Client Systems Technician (CST), helpdesk or any person with administrator or elevated privilege rights.

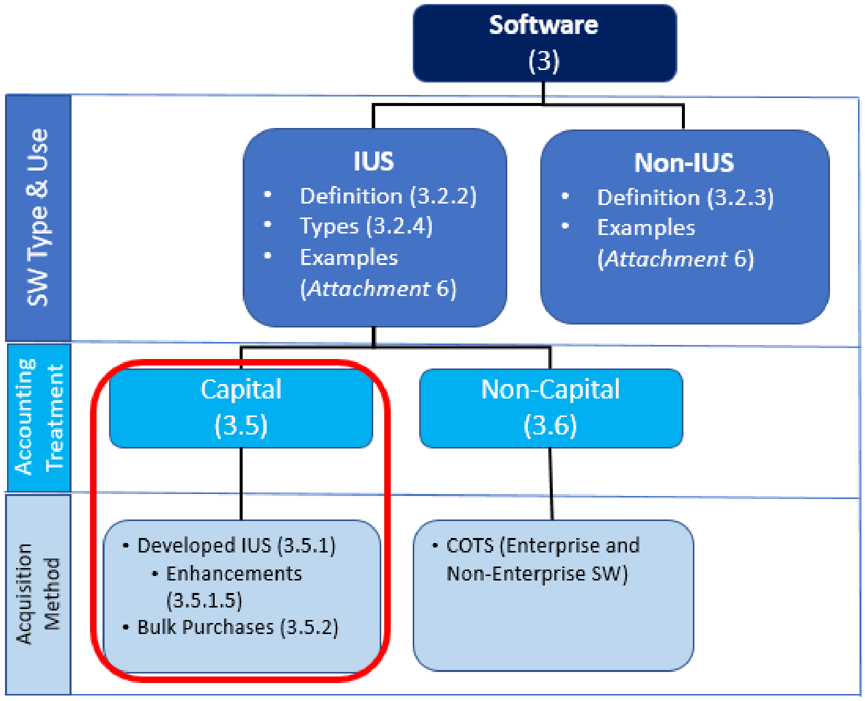
3.4.2.8.18. Does not purchase, obtain, or install hardware or software without prior coordination with the applicable USLM. **(T-3)**.

3.4.2.8.19. Notifies USLM (or equivalents) of any actions performed that changes local software licenses installed on computer systems. Must maintain a record of and notify USLMs when installing software from shared folders or using installation CDs/DVDs. Also maintain a record of and notify USLM (or equivalents) when uninstalling, upgrading, or performing any actions that change the amount or number of licensed software products installed on the network. Ensure software covered by an ELA is not transferred with hardware that is being replaced or repurposed outside of the ELA scope. **(T-3)**.

3.4.2.8.20. Ensures that only software listed on an approved products list is installed, in accordance with AFI 17-130, and Products Approval Process Memo signed on 1 June 2015 by Brigadier General Wootton. Approved sources are the Air Force Evaluated/Approved Products Listing (E/APL), and the Air Force Authorizing Official SW Cert Resources for Reciprocity. For Air Force/A2/6 systems, the Air Force IC APL is maintained at https://intelshare.intelink.gov/sites/Air Forceisra-a6s/a6sc/Lists/APL/AllItems.aspx. **(T-1)**.

3.5. Capital Internal Use Software Accountability and Management.

Figure 3.5. Capital Internal Use Software Lifecycle Guidance.



3.5.1. Developed Internal Use Software Lifecycle.

3.5.1.1. General Definition and Requirements.

3.5.1.1.1. Developed IUS is software that has been internally developed by the Air Force, including new software that is modified with or without a contractor's assistance; or contractor-developed software that Air Force paid a contractor to design, install and implement, including new software or modification of existing software.

3.5.1.1.2. This section outlines steps and prescribes processes for acquisition, development, management, sustainment, enhancement and disposal of contractor-developed or modified software.

3.5.1.1.3. The capitalized cost of contractor-developed software shall include the amount paid to the contractor to design, program, install, and implement new software or to modify existing software, including labor, plus any costs incurred during development and implementation (such as training, administration, and testing of software). **(T-0).**

3.5.1.1.4. Guidance related to process for capturing labor cost for software that was developed or modified by Air Force personnel (military and civilian labor), will be addressed in the future iteration of this manual.

3.5.1.1.5. For additional information, refer to DOD FMR, volume 4, chapter 27.

3.5.1.2. Acquisition and Procurement Process.

3.5.1.2.1. The CO will write the contract in conjunction with the PM, per requirements detailed in **Table 3.1** and ensure the application of uniform CLIN structure for IUS to facilitate properly Developed IUS cost estimates is in accordance with Defense Federal Acquisition Regulation System (DFARS) Procedures, Guidance, and Information (PGI), 204.7103 - Contract Line Items and DOD FMR, Volume 4, chapter 27. **(T-0)**.

3.5.1.2.2. Additionally, when procuring IUS, Air Force contracting activities will:

3.5.1.2.3. Ensure uniform CLIN and SLIN structure for IUS is used when procuring IUS, and that IUS requirements are on CLIN(s) separate from other requirements as defined in the requirement document(s). **(T-1)**.

3.5.1.2.4. Ensure that the CLIN and SLIN structure aligns with the lines of accounting for capital and non-capital expenditures as outlined in **Table 3.1. (T-1)**.

3.5.1.2.5. Ensure that the appropriate solicitation instructions, provisions contract clauses and CDRL are included in solicitations and contract awards as applicable. **(T-1)**.

3.5.1.2.6. Ensure instructions for contractors to identify any IUS desired and required for performance as well as ownership, deliverables and licenses for the effort that are in the contract.

3.5.1.2.7. Ensure contracts for the development of IUS include a listing of all contractor supplied IUS.

3.5.1.2.8. Ensure that the requiring activity has discussed the types and approximate quantities of IUS required and included them in acquisition plans/strategy documents, and requirements packages.

3.5.1.2.9. Ensure coordination with the Functional Owner (FO) to review all approved contractor requests to purchase and/or develop IUS where the Government will retain the title. **(T-1)**.

3.5.1.2.10. For non-Defense Contract Management Agency (DCMA) administered firm fixed price contracts, ensure that invoices contain the contract line item level detail.

Table 3.1. Internal Use Software Capitalization Cost Determination.

Project Phase	Task	Treatment
Concept Planning, Planning and Requirements	Project evaluation	Expense
	Concept testing	Expense
	Evaluation of alternatives	Expense
	Project approval	Expense
Design, Development and Testing, Implementation	Design, including software configuration and software interfaces	Capitalize
	Coding	Capitalize
	Installation to hardware	Capitalize
	Project personnel costs	Capitalize
	Testing	Capitalize
	Quality assurance testing	Capitalize
	Documentation	Capitalize
	General and admin costs	Allocate
	Data conversion software	Expense
Operations & Maintenance, Disposition	Training	Expense
	Data conversion	Expense
	Help Desk	Expense
	Enhancements	Case by case evaluation
	Maintenance, bug fix	Expense

3.5.1.3. Development Process.

3.5.1.3.1. Within 7 calendar days upon start of IUS development activities, PMO/FO must notify DPAS PA to establish IUS in Development catalog item in DPAS, as per detailed instructions outlined in DPAS Quick Reference Guide (QRG). **(T-2)**.

3.5.1.3.2. Upon receiving of vendor invoices, the PMO/COR will validate that the invoices received conform to the terms of the contract regarding Developed IUS CLIN and CDRL identifications. The COR will do the following in determining whether to approve or reject invoice in Invoicing, Receipt, Acceptance and Property Transfer. **(T-2)**:

3.5.1.3.3. Ensure that CDRL information, as defined during contracting activities is reported by the vendor.

3.5.1.3.4. Ensure that CLIN information, as defined during contracting activities, will be reported by the vendor and included in the submitted invoice. **(T-2)**.

3.5.1.3.5. If vendor provided invoice does not reflect CLIN structure as defined in **Table 3.1**, COR or PM will reject the invoice and request that vendor corrects invoice data and resubmit the invoice for processing. **(T-2)**.

3.5.1.3.6. Within 7 calendar days of receiving an acceptable invoice, PM will provide the invoice to designated DPAS PA. **(T-2)**.

3.5.1.3.7. Upon receipt of the initial approved invoice, DPAS PA will follow instructions outlined in DPAS QRG to establish CIP project for developed IUS in DPAS. **(T-2)**.

3.5.1.3.8. On a quarterly basis, but no later than 7 calendar days prior to the end of a reporting period, DPAS PA will populate Air Force Form 7500, *Internal Use Software Cost Tracking,* as prescribed in **Attachment 8**, with valid developed IUS cost data and add spent cost to DPAS IUS in Development record with the applicable KSDs. **(T-2)**.

3.5.1.3.9. Air Force Form 7500 might include:

3.5.1.3.9.1. Full non-government personnel labor costs (vendor cost) incurred during the software development stage as outlined in **Table 3.1**.

3.5.1.3.9.2. COTS software cost that was purchased exclusively for modification.

3.5.1.3.9.3. COTS software used exclusively in the development of IUS.

3.5.1.3.9.4. Software license costs for software used exclusively in the development of IUS.

3.5.1.3.9.5. Regardless of the bulk criteria, all COTS software licenses procured to be a component of developed IUS will be included in the DPAS asset record of a parent developed IUS. **(T-2)**.

3.5.1.3.10. AF Form 7500 should not include the following cost:

3.5.1.3.10.1. Data conversion cost: costs incurred to develop or obtain software that allows for access or conversion of existing data to the new software are expensed as incurred. Such costs may include the purging or cleansing of existing data, reconciliation or balancing of data, and the creation of new or additional data. To the extent data conversion costs are used to obtain data exclusively to support development, they may be capitalized as development costs.

3.5.1.3.10.2. Training costs: post-deployment training costs.

3.5.1.3.10.3. Cost incurred solely to repair a design flaw or to perform minor upgrades that may extend the useful life of the software without adding capabilities must be expensed. **(T-0)**.

3.5.1.3.10.4. Government or civilian labor cost incurred during the software development phase will not be captured at this time. Instructions for capturing this type of labor will be provided during the next iteration of this policy.

3.5.1.3.11. Allocation of cost to the IUS in development account will stop when the MDA declares that Capability Support ATP has been met, as described in DODI 5000.75, *Business Systems Requirements and Acquisition*. **(T-0)**.

3.5.1.3.12. MDA will determine when if the program is justified for limited deployment (LD) or full deployment (FD) and signs the appropriate Decision Memo (LDD or FDD). Through the signed Limited Deployment Decision (LDD) or FDD, the MDA will communicate the approval to the PMO. **(T-2)**.

3.5.1.3.13. PM/FO will obtain Deployment Decision Memo (DDM) from MDA and within 7 days of attaining the memo or within the same reporting period if less than 7 days, PM will provide (DDM) to DPAS PA. **(T-2)**.

3.5.1.3.14. Within 7 calendar days of attaining the memo but within the same reporting period if less than 7 calendar days, DPAS PA will follow DPAS QRG to update IUS in development record in DPAS to indicate that development activities have ended. **(T-2)**.

3.5.1.3.15. DPAS PA will inform DPAS APO of IUS lifecycle change from IUS in development to IUS in service. **(T-2)**.

3.5.1.3.16. Please refer to **Attachment 6**, **figure 6.1.** *Developed IUS Acquisition and Development process* flowchart.

3.5.1.4. Management/Sustainment Process.

3.5.1.4.1. Accountability for developed IUS will begin at the end of the development phase and placed in service date will be established when DDM is signed by MDA. **(T-1)**.

3.5.1.4.2. The DPAS PA will follow DPAS QRG to receive an asset and create IUS asset entry in DPAS. **(T-1)**.

3.5.1.4.3. The DPAS PA will maintain accountability of IUS records for the life of the asset. **(T-1)**.

3.5.1.4.4. The DPAS PA will update asset record for any changes to the status of the IUS asset such as enhancements, transfer or disposal. **(T-1)**.

3.5.1.4.5. The DPAS PA will inform DPAS APO about any changes in the status of the IUS asset throughout its lifecycle. **(T-1)**.

3.5.1.4.6. The DPAS PA will maintain all required KSDs and respond to inventory and audit requests within 7 calendar days of request, as prescribed in DODI 5000.76. **(T-0)**.

3.5.1.5. IUS Enhancement Process.

3.5.1.5.1**.** Accountable organization DPAS PA responsible for the IUS asset will monitor the asset for potential enhancement activities. **(T-1)**.

3.5.1.5.2. There are two types of software enhancements and only major enhancements types will be capitalized by the Air Force. **(T-0)**.

3.5.1.5.3. A major IUS enhancement is a modification to existing IUS that provides it with significant additional capabilities and enables the software to perform tasks that it was previously incapable of performing. As stated in the Statement of Federal Financial Accounting Standards (SFFAS) 10: *Accounting for Internal Use Software*, para 26, major enhancements normally require new software specifications and may require a change to all or part of the existing software specifications. Examples of major enhancements could include augmenting existing business functions with new features, and/or adding new functionality and capability.

3.5.1.5.4. DPAS PA will monitor and track all capital enhancements in DPAS that add new capabilities based on the following criteria. **(T-1)**:

3.5.1.5.4.1. It is more likely than not that the enhancements will result in significant increase in capabilities and functionality that is visible to the user; that is, modifications to enable the IUS to perform tasks that it was previously incapable of performing.

3.5.1.5.4.2. Costs equal to or exceeding the current capitalization threshold ($250K or more).

3.5.1.5.4.3. The enhancement has an expected service life of 2 years or more.

3.5.1.5.5. A minor enhancement is one that has no impact on the overall capability or functionality of the system. The cost of minor enhancements will not be reported in DPAS and will be expensed in the period incurred. **(T-0)**. Examples of minor enhancements include updating data tables, web-enabling, customizing reports, or changing graphic user interfaces. Additionally:

3.5.1.5.5.1. Software upgrades that are included in annual maintenance and security assurance agreements must be expensed, not be capitalized as enhancements or separate assets. **(T-0)**.

3.5.1.5.5.2. Costs incurred solely to repair a design flaw or to perform minor upgrades that may extend the useful life of the IUS without adding capabilities will not be capitalized and must be expensed. **(T-0)**. However, the useful life of the IUS is subject to adjustment and must reflect the enhancement. **(T-0)**.

3.5.1.5.5.3. Enhancements that extend the useful life of the software without adding significant capabilities are to be considered minor enhancements and must be expensed. **(T-0)**. However, in instances where the useful life of the software is extended, the amortization period must be adjusted as described. **(T-0)**.

3.5.1.5.6**.** The purchase of enhanced versions of software that do not meet capitalization criteria must be expensed in the period incurred. **(T-0)**.

3.5.1.5.7. If it is determined that enhancement falls under the major enhancement category, DPAS PA should perform the same steps that are outlined in **paragraph 3.5.1.3.** of this guidance. **(T-1)**.

3.5.1.5.8. Each enhancement will be reported separately with the capital threshold applicable to the overall development effort, not each increment. **(T-0)**.

3.5.1.5.9. Any increments following the initial deployment will be accounted for as a separate IUS enhancement. **(T-0)**.

3.5.1.6. IUS Transfer Process.

3.5.1.6.1. When IUS asset ownership changes from one accountable organization to another, DPAS PA of the owning organization will initiate the transfer in DPAS following the steps outlined in DPAS QRG. **(T-1)**.

3.5.1.6.2. When transferring the asset, DPAS PA will make sure that all documentation applicable to the lifecycle of that asset (e.g., acquisition documentation, invoices, etc.) is transferred to the gaining organization, whether internal or external to the Air Force. **(T-1)**.

3.5.1.6.3**.** Full guidance on transfer requirements can be found in the DOD FMR, volume 4, chapter 27, section 270203 paragraph G.2.

3.5.1.7. IUS Disposal Process.

3.5.1.7.1. To properly transfer, dispose of, donate, or reuse commercial IUS, accountable organizations must adhere to product licensing agreements to avoid potential fines or litigation. **(T-0)**.

3.5.1.7.2. Accountable organizations must consult all relevant parties before any IUS disposition activity. **(T-2)**.

3.5.1.7.3. Upon disposal, accountable organization DPAS PA will remove the asset from DPAS and inform the DPAS APO. **(T-1)**. This will include a statement verifying that all media, licenses, and documentation have been destroyed or returned to the vendor. **(T-1)**.

3.5.2. Bulk Purchases Lifecycle.

3.5.2.1. Bulk Purchases Lifecycle Process.

3.5.2.1.1. Bulk purchases are purchases of COTS software programs that meet criteria describes in **paragraph 3.5.2.2.2**.

3.5.2.1.2. This section prescribes process for and steps for acquisition, sustainment and disposal of bulk purchases.

3.5.2.1.3. For additional information on accountability and management of non-capital IUS, please refer to DODI 5000.76 and DOD FMR, Volume 4, Chapter 27.

3.5.2.2. Acquisition Process.

3.5.2.2.1**.** All software will be procured using applicable buying programs as prescribed in **paragraph 3.6.1.1**.

3.5.2.2.2. The BSLM will monitor acquisition of bulk software purchases and establish a single asset record in DPAS if purchase meets all of the following criteria. **(T-1)**:

3.5.2.2.2.1. The purchase is made on the same procurement transaction or purchase order **and** under the same manufacturer part number or stock keeping unit (SKU). **(T-1)**.

3.5.2.2.2.2. The software license part number or SKU is for a *new perpetual license*, or a term license (new or renewal) with a license term of greater than two years. **(T-1)**.

3.5.2.2.2.3. The total combined funds expended by the owning organization (unit) for the bulk purchase cost for the same licenses (SKU) reaches the bulk-purchase capitalization threshold ($250,000 or more). **(T-1)**.

3.5.2.2.3. If the COTS software licenses are purchased for use in or integration with Developed IUS, regardless of purchase cost or if they meet bulk purchased criteria, Developed IUS processes in **paragraph 3.5.1.1** will apply. **(T-1)**.

3.5.2.3. Sustainment Process.

3.5.2.3.1**.** The DPAS BSLM will establish a single DPAS asset record for software bulk purchase that meets criteria described in **paragraph 3.5.2.2.2.,** for each distinct manufacture part number or SKU, sum the quantities ordered and assign unique identification as prescribed in DPAS QRG. **(T-2)**.

3.5.2.3.2. To determine the total cost amount for individual bulk purchase record, only software licenses cost should be included (cost for software maintenance should be excluded from the total calculation).

3.5.2.3.3. The BSLM will maintain bulk purchase accountable asset record for the life of the software license in accordance with the terms of the license agreement. **(T-2)**.

3.5.2.3.4. The BSLM will retain all KSDs that pertain to the bulk asset record in accordance with DODI 5000.76. **(T-0)**.

3.5.2.4. Disposal.

3.5.2.4.1. The BSLM will dispose of software in accordance with license agreements and/or by the following methods. **(T-2)**:

3.5.2.4.1.1. Return the software package (distribution media, manuals, etc.) to the company that developed the software.

3.5.2.4.1.2. Destroy the software and license keys according to the provisions of the licensing agreement.

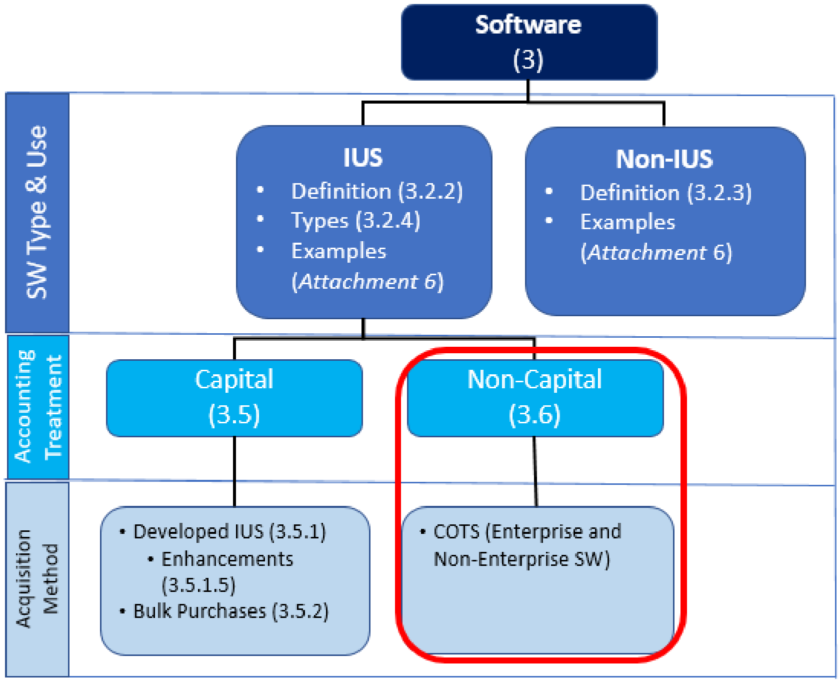
3.5.2.4.1.3. Document the method of destruction to establish an audit trail.

3.5.2.4.1.4. Disposal is not complete unless all copies of the decommissioned IUS are uninstalled from the network through uninstall procedures or proper disposition of the computer hardware or hard drive upon which the software is installed.

3.5.2.4.2. Upon disposal, BSLM will remove the asset record from DPAS and inform the DPAS APO of the disposal. This will include a statement verifying that all media, licenses, and documentation have been destroyed or returned to the vendor. **(T-2)**.

3.6. Non-Capital IUS Accountability and Management.

Figure 3.6. Non-Capital IUS Lifecycle Guidance.



3.6.1. Non-Capital IUS types.

3.6.1.1. Software that is procured and managed as a component of Air Force ELA or JELA will be referred to as enterprise software throughout this section.

3.6.1.2. Software that is not managed as a component of an ELA, JELA or provided from the Air Force standard desktop configuration (SDC), will be referred to as non-enterprise software.

3.6.2. Non-Capital IUS Lifecycle Process.

3.6.2.1. This section prescribes processes and outlines steps for acquisition, management, sustainment, inventory and disposal of non-capital IUS.

3.6.2.2. For additional information on accountability and management of non-capital IUS, please refer to DODI 5000.76 and DOD FMR, Volume 4, Chapter 27.

3.6.3. Acquisition Process.

3.6.3.1. All Air Force software will be procured using applicable buying programs (in order of precedence):

3.6.3.1.1. Air Force ELA. **(T-1)**.

3.6.3.1.2. DOD/JELA. **(T-1)**.

3.6.3.1.3. DOD Enterprise Software Initiative (ESI) blanket purchase agreements. **(T-1)**.

3.6.3.1.4. General Services Administration (GSA) 2GIT Blanket Purchase Agreement schedules. **(T-1)**.

3.6.3.1.5. If no current ELA/JELA exists for the required software category, BSLM/USLM will contact IT-BAO to perform an analysis for ACC to make determination if new ELA/JELA needs to be established. **(T-1)**.

3.6.3.1.6. Other vendor-authorized sources. **(T-1)**.

3.6.3.2. The USLM will serve as the unit focal point for all software acquisition for the unit. **(T-1)**.

3.6.3.3. Prior to purchasing enterprise software, USLM will coordinate all enterprise software acquisitions through the respective BSLM and SBA (or equivalent). **(T-1)**.

3.6.3.4. Prior to purchasing non-enterprise software, USLM will coordinate software acquisitions through the respective BSLM (or equivalent). **(T-1)**.

3.6.3.5. To ensure that proper accountability can be performed on the purchased license(s), documentation verifying the acquisition cost of the license(s) will be retained by the acquiring or accountable organization USLM and/or BSLM. **(T-1)**.

3.6.3.6. Documentation may include, but is not limited to; GPC receipts, purchase orders, contract agreements, license keys, documentation of entitlements, End User License Agreement, contract clauses and other procurement and contract documentation.

3.6.3.7. The USLM and/or BSLM must retain proof of software purchase and proof of government rights to the software, regardless of dollar value of the purchase. **(T-0)**.

3.6.3.8. Refer to **Attachment 7**, **figure 7.1**, and **figure 7.2**.

3.6.4. Management Process/Sustainment.

3.6.4.1. The USLM will create asset record in local repository or a managerial system within 7 working days of receipt and acceptance by the government or by the end of the calendar month, whichever is shorter. **(T-0)**.

3.6.4.1.1. The USLM will ensure that the licenses that are no longer needed by the intended user are removed from their system and retained for future use/deployment (e.g., transfer of the user to new program, no longer a validated need). **(T-1)**.

3.6.4.1.2. The USLM will maintain software assets records owned by the organization in the managerial system or local repository for the life of the software asset. **(T-1)**.

3.6.4.1.3. The USLM/BSLM will utilize automated network scanning to the maximum extent possible for tracking software installed on the base network where applicable. **(T-1)**.

3.6.4.1.4. The USLM might initiate redistribution of excess or superseded software if:

3.6.4.1.4.1. It is permitted under the license agreement or upgrade policy for that software.

3.6.4.1.4.2. Software is not classified.

3.6.4.1.4.3. Software did not provide direct security protection to systems that processed classified information.

3.6.4.1.4.4. Software is not directly related to or associated with a weapon system, intelligence system, command and control system, communications system, or tactical system.

3.6.4.1.4.5. It still operates as intended.

3.6.4.1.4.6. The asset record, and all documentation associated with it, must be transferred to the gaining organization along with the asset. **(T-0)**.

3.6.4.1.5. USLM/BSLM will audit all systems to ensure no illegal or unauthorized copies of software are installed. Sampling procedures may be used if active inventorying/auto discovery systems are available. **(T-1)**.

3.6.4.1.6. BSLM and ESLM will monitor legal use of enterprise licenses to ensure usage does not exceed quantities purchased. **(T-0)**.

3.6.5. Inventory Process.

3.6.5.1. USLM will inventory all non-enterprise software annually or as requested and, if available utilize network scanning and monitoring tools, e.g., SCORE, Tanium ®, SCCM, CMDB, to track and report installed software and license information, as prescribed in DODI 5000.76. **(T-0)**.

3.6.5.1.1. USLM will conduct annual inventory for enterprise software that is installed on stand-alone devices, as prescribed in DODI 5000.76. **(T-0)**.

3.6.5.1.2. BSLM will assist ESLM in performing annual inventory of enterprise software licenses and reconcile them against contract information to maintain accountability of what the government has purchased as well as to ensure adherence to legal use per contract term. **(T-1)**.

3.6.5.1.3. USLM will conduct inventory 30 days from date of appointment and/or 1 year from the date of the last inventory, whichever comes first. **(T-1)**.

3.6.5.1.4. USLM will provide annual inventory to the UAPO for approval. **(T-1)**.

3.6.5.1.5. UAPO will certify annual inventory with a handwritten or digital signature indicating completion of the inventory and submit to the BSLM (or equivalents). **(T-0)**.

3.6.5.1.6. BSLM will retain proof of conducted annual inventory for audit purposes and provide to higher headquarters and auditors if requested, as prescribed in DODI 5000.76. **(T-0)**.

3.6.5.1.7. Refer to **Attachment 7**, **figure 7.3**.

3.6.6. Disposal Process.

3.6.6.1. The USLM will dispose of software in accordance with license agreements and/or by the following methods:

3.6.6.1.1. Return the software package (distribution media, manuals, etc.) to the company that developed the software. **(T-1).**

3.6.6.1.2. Destroy the software and license keys according to the provisions of the licensing agreement and document the method of destruction to establish an audit trail. **(T-1).**

3.6.6.2. Ensure all copies of the decommissioned IUS are uninstalled from the network through uninstall procedures or proper disposition of the computer hardware or hard drive upon which the software is installed. Disposal is not complete unless these actions are taken. **(T-1).**

3.6.6.3. USLM will document the destruction, or vendor return, and update IUS record in local repository or a managerial system. **(T-1)**.

3.6.6.4. USLM will retain all of the KSDs to show evidence of the disposal. This will include a statement verifying that all media, licenses, and documentation have been destroyed or returned to the vendor. **(T-1)**.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

10 USC § 2464, *Core logistics capabilities.*

10 USC § 2466, *Limitations on the performance of depot-level maintenance of materiel.*

31 USC §§ 901-903, *Chief Financial Officers (CFO) Act of 1990*

DFARS PGI 204.7103, *Contract Line Items*, current edition.

Executive Order 13589, *Promoting Efficient Spending*.

National Security Agency/Central Security Service Policy Manual 9-12, *NSA/CSS Storage Device Sanitization Manual*, December 15, 2014.

NARA Directive 1571, *Archival Storage Standards*, 15 February 2002.

DAFPD 17-1, *Information Dominance Governance and Management*, 12 April 2016.

DAFPD 17-2, *Cyberspace Operations*, 12 April 2016.

DAPFD 10-6, *Capability Requirements Development*, 6 November 2013.

DAFI 33-360, *Publications and Forms Management*, 1 December 2015.

FAR Subpart 7.5, *Inherently Governmental Functions*, current edition.

DOD FMR 700.14-R, Volume 1, Chapter 9, *Financial Records Retention*, February 2016.

DOD FMR 700.14-R, Volume 3, Chapter 8, *Standards for Recording and Reviewing Commitments and Obligations*, February 2020.

DOD FMR, 7000.14-R, Vol 4, Chapter 25, *General Equipment*, May 2019.

DOD FMR, 7000.14-R, Vol 4, Chapter 27, *Internal Use Software*, August 2018.

DOD FMR 7000.14-R, Volume 12, Chapter 7, *Financial Liability for Government Property Lost, Damaged, Destroyed, or Stolen*, March 2014.

DODI 4151.19, *Serialized Item Management (SIM) for Life-Cycle Management of Materiel*, 9 January 2014.

DODM 4160.21, Volume 2*, Defense Materiel Disposition: Property Disposal and Reclamation*, 22 October 2015.

DODI 5200.01, DOD Information Security Program and Protection of Sensitive Compartmented Information (SCI), 21 April 2016.

DODI 5000.02, *Operation of Adaptive Acquisition Framework*, 23 January 2020.

DODI 5000.64, *Accountability and Management of DOD Equipment and Other Accountable Property*, 27 April 2017.

DODI 5000.75, *Business Systems Requirements and Acquisition*, 2 February 2017.

DODI 5000.76, *Accountability and Management of Internal Use Software (IUS)*, 7 June 2019.

DODI 8320.04, *Item Unique Identification (IUID) Standards for Tangible Personal Property*, August 27, 2019.

SFFAS 10: *Accounting for Internal Use Software*, 9 October 1998.

AFI 16-1404, *Air Force Information Security Program*, 29 May 2015.

AFI 17-130, *Cybersecurity Program Management*, 13 February 2020.

AFI 21-103, *Equipment Inventory, Status, and Utilization Reporting*, 30 April 2020.

AFI 23-111, *Management of Government Property in Possession of the Air Force*, 19 November 2018.

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020.

AFI 38-101, *Manpower and Organization*, 29 August 2019.

AFI 63-101/20-101, *Integrated Life Cycle Management*, 30 June 2020.

AFI 65-201, *Managers' Internal Control Program Procedures*, 9 February 2016.

AFMAN 14-403, *Sensitive Compartmented Information Security and Intelligence, Surveillance, and Reconnaissance Systems Cybersecurity and Governance*, 3 September 2019.

AFMAN 17-1301, *Computer Security (COMPUSEC)*, 12 February 2020.

Prescribed Forms

Air Force Form 7500, *Internal Use Software Cost Tracking*

Adopted Forms

DD Form 200, *Financial Liability Investigation of Property Loss*

DD Form 1149, *Requisition and Invoice/Shipping Document*

DD Form 3041, *Accountable Property System of Record (APSR) Requirements Checklist for Internal Use Software (IUS)*

DD Form 1348-1A, *Issue Release/Receipt Document*

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

ACC - Air Combat Command
AF – Air Force
AFECO - Air Force Equipment Control Officer
AFI - Air Force Instruction
AFMAN – Air Force Manual
AFMC – Air Force Material Command
AIT - Automated Identification Technology
APIAW - Accountable Property Inventory Adjustment Worksheet
APO - Accountable Property Officer
APR- Accountable Property Records
APSR - Accountable Property System of Record
AR - Accountability Record
ATP - Authority to Proceed
AU - Assessable Unit
AUIC - Accountable Unit Identification Codes
BPA- Blanket Purchase Agreement
BSLM - Base Software License Manager
CAGE - Commercial and Government Entity code
CCC - Cyberspace Capabilities Center
CDRL - Contract Data Requirements List
CIP – Construction in Progress
CLIN - Contract Line Item Number
CO – Contracting Officer
COR - Contracting Officer Representative
COTS - Commercial Off-the-Shelf
CST - Client Systems Technician
DAFI – Department of the Air Force Instruction
DAFPD - Department of the Air Force Policy Directive
DLA - Defense Logistics Agency
DLADS - Defense Logistics Agency Disposition Services
DOD - Department of Defense
DOD FMR - Department of Defense Financial Management Regulation

DODD - Department of Defense Directive

DODI - Department of Defense Instruction

DOLI - Date of last inventory

DPAS - Defense Property Accountability System

DPI - Digital Printing & Imaging

DRMS - Defense Reutilization and Marketing Service

DRU - Direct Reporting Unit

E/APL – Evaluated/Approve Products List

ECO - Equipment Control Officer

ELA - Enterprise License Agreement

ESI - Enterprise Software Initiative

ESLM - Enterprise Software License Manager

FAR - Federal Acquisition Regulation

FDD - Full Deployment Decision

FECO - Functional Equipment Control Office

FO – Functional Owner

FOA - Field Operating Agency

FOB - Found-on-Base

GE – General Equipment

GFP - Government Furnished Property

GPC – Government Purchase Card

GSA - General Services Administration

GSU - Geographically Separated Units

HTSA - Host Tenant Support Agreement

HW - Hardware

IA - Information Assurance

IO – Information Owner

ISR - Intelligence, surveillance, and reconnaissance

ISSO - Information System Security Officer

IT - Information Technology

IT BAO - Information Technology Business Analytics Office

ITAM - Information Technology Asset Management

ITCC - IT Commodity Council

ITIPS - IT Investment Portfolio System

IUID - *Item Unique Identification*

IUS - Internal Use Software

JELA - Joint Enterprise License Agreements

KSD – Key Supporting Document

LDD - Limited Deployment Decision

MAJCOM - Major Command

MDA - Milestone Decision Authority

MOA - Memorandum of Agreement

MPS - Managed Print Services

ODNI - Office of the Director of National Intelligence

OPR - Office of Primary Responsibility

PA – Property Administrator
PC - Property Custodians
PM – Program/Project Manager
PMO – Program Management Office
POC - Point of Contact
PSM - Product Support Manager
QRG - Quick Reference Guides
RFP - Request for Proposal
ROS - Reports of Survey
SaaS - Software as a Service
SAE - Service Acquisition Executive
SAP - Special Access Program
SBA - Software Benefits Administrator
SCIF - Sensitive Compartmented Information Facility
SCR - System Change Requests
SEAMLS - Software Enterprise Acquisition Management Lifecycle Support
SFFAS - Statement of Federal Financial Accounting Standards
SIM - Serialized Item Management
SKU - Stock Keeping Unit
SLIN - Sub-line numbering
SW - Software
UAPO - Unit Accountable Property Officer
UIC - Unit Identification Codes
USLM - Unit Software License Manager
WCO - Wing Cybersecurity Office
WPAN - Wireless Personal Area Network

Terms

Accountable Property - Property that meets accountability requirements as prescribed in DODI 5000.64 and 5000.76 is recorded in the designated APSR, which is DPAS for the Air Force.

The Defense Property Accountability System (DPAS) – A Department of Defense (DOD) property management system.

Enterprise Software Initiative (ESI) - is a contract mechanism that establishes and manages COTS IT agreements, assets, and policies for the purpose of lowering total cost of ownership across the DOD, Coast Guard and Intelligence communities.

Internal Use Software - A stand-alone application, or the combined software components of an IT system that can consist of multiple applications, modules, or other software components integrated and used to fulfill an internal or operational need. Software acquired or developed to meet internal or operational needs. Software used to operate Air Force programs (e.g., financial and administrative software). Software used to produce goods and provide services (e.g., maintenance work order management).

Functional Equipment Control Officer (FECO) - An individual appointed by a FOA, DRU, or equivalent that oversees the management and control of IT assets within their area of responsibility.

Serialized Item Management - The assignment and marking of individual assets with a standardized, machine-readable, two-dimensional marking containing a globally unique and unambiguous item identifier to improve the Air Force's capability to manage materiel through the generation, collection, and analysis of data on individual assets in order to enhance asset visibility and financial accountability and to improve system life cycle management

Service Owner – This person accountable for one or more services throughout their entire service lifecycle, regardless of where the technology components, processes or professional capabilities reside. The Service Owner is a single point of accountability in front of the customer for all aspects of a dedicated service. This role has the authority and responsibilities to ensure that activities are performed to identify, document and fulfill service requirements.

ATTACHMENT 2

DESIGNATED APSR GUIDANCE

A2.1. Purpose and Scope. This attachment provides guidance for use of the designated APSR. SAF/CN has designated Defense Property Accountability System (DPAS) as the Accountable Property System of Record for IT hardware assets. The DPAS Site ID is FF-GEIT. Additional guidance will be provided by Air Force/A2/6 for SCI and national ISR assets.

A2.2. DPAS Roles and Responsibilities. The table below identifies DPAS roles and the corresponding Air Force personnel as prescribed in **paragraph 1.2**.

Table A2.1. Crosswalk of roles in DPAS and roles prescribed in paragraph 1.2.

DPAS Role	Air Force Role
Accountable Property Officer (APO)	AFECO
Property Administrator (PA)	FECO, ECO
Property Custodian (PC)	PC
Information Owner (IO)	AFECO
Data Inquiry	AFECO, FECO, ECO, PC, Auditors
Forms and Reports	AFECO, FECO, ECO, PC, Auditors

Table A2.2. Crosswalk of DPAS site structure and existing Air Force structure.

DPAS Structure	Air Force Structure
AUIC	DODAAC
UIC	Unit
Custodian Number	Account Number

A2.2.1. Information Owner (IO).

A2.2.1.1. Approves and processes new user access requests and submits access request packages to DPAS Security for account creation and update.

A2.2.1.1.1. The AFECO is the IO for DPAS and must review/approve all access requests for Property Administrators and Auditors. Requesting access to DPAS must be accomplished via the AFECO SharePoint site. This site will provide an access request module containing all necessary instructions, forms, and routing procedures.

A2.2.1.2. Reviews/approves/submits new role requests for ECO/FECO/Auditors to DPAS for approval.

A2.2.1.2.1. Users requesting a new role be added or updated must submit a Role Request Form to the IO.

A2.2.1.3. Serves as the Catalog Manager to standardize the catalog and create new catalog records for each unique Stock Number, Manufacturer Name, Model Number, and Manufacturer CAGE Code combination.

A.2.2.1.4. Will review, validate, and process System Change Requests (SCR) for DPAS when issues are identified by the PA.

A2.2.2. Accountable Property Officer (APO).

A2.2.2.1. Will add, update, or delete Accountable Unit Identification Codes (AUIC) across the enterprise as necessary. **(T-1).**

A2.2.3. Property Administrator (PA).

A2.2.3.1. Will request access to DPAS via the AFECO SharePoint site and then maintain access for their tenure as PA. **(T-1).**

A2.2.3.2. Must be at least E-5 or GS-7 rank to perform the duties. **(T-1).**

A2.2.3.3. Receives and enters new asset records into DPAS via the Asset Receiving function.

A2.2.3.4. Processes receipt, transfer, and disposition of all IT assets in DPAS.

A2.2.3.4.1. Ensures appropriate documentation is generated and attached to asset transfers from UIC to UIC and/or custodian to custodian (DD Forms 1149, 1140, 1348-1A).

A2.2.3.4.2. Ensures assets on loan to a contractor be classified as GFP.

A2.2.3.4.2.1. Classifies GFP on loan with DPAS Loan Code “C” =Out on Loan to Non-Government Activity until asset is returned. (Note: If asset is loaned to a specific Contractor, be sure to identify the Contract Number from the DPAS drop down list to select the corresponding Contract.)

A2.2.2.4.3. Designates and allocates excess assets.

A2.2.3.5. Ensures an appropriate KSD is attached to every asset transaction using the attachment data field associated with the asset record in accordance with **Attachment 4**.

A2.2.3.6. Ensures all non-capital assets are entered into DPAS with Fund Code “99” and Capital Code “A”.

A2.2.3.6.1. Ensures all capital assets are entered into DPAS with the corresponding Fund Code and Interface System Code “AG”.

A2.2.3.7. Add, update, or delete Unit Identification Codes (UIC) as necessary within their area of responsibility.

A2.2.3.8. Add, update, or delete custodian accounts as necessary within their area of responsibility.

A2.2.3.9. Request new catalog records to the DPAS Catalog Manager/AFECO via the AFECO ITAM DPAS SharePoint site.

A2.2.3.10. Will ensure all assets entered into DPAS have been coded only with one of the following four condition codes:

“A”=Active in use or slotted for use (e.g., new unit standing up)
“C”=Serviceable excess not in use (overage above spares)
“J”=Serviceable Spare
“K”=Ready for turn in to DLADS

A2.2.4. Property Custodian (PC).

A2.2.4.1. Conducts and completes inventories for assets within their account.

A2.2.4.2. Ensures all assets are affixed with a barcode label that includes the asset’s Serial Number, Part Number, and Manufacturer CAGE Code.

A2.2.5. Data Inquiry.

A2.2.5.1. Generate pre-defined and custom queries within FF-GEIT.

A2.2.6. Forms and Reports.

A2.2.6.1. Generate reports in DPAS for their area of responsibility.

ATTACHMENT 3

IT HARDWARE ENTERPRISE INVENTORY PLAN.

A3.1. Purpose and Scope.

A3.1.1. The intent of this plan is to articulate the minimum requirements for performing asset/item inventories for IT hardware assets. Additional requirements that may be levied onto units by their parent MAJCOM/DRU/FOA organization will be articulated in a MAJCOM/DRU/FOA-specific Inventory Plan. Additional guidance may be provided by Air Force/A2/6 for SCI and national ISR assets.

A3.2. Inventory Frequency.

A3.2.1. All Hardware Assets meeting the criteria stated in **paragraph 2.4.3.** and **2.4.4.** will be inventoried annually.

A3.3. Preparing for Inventory.

A3.3.1. To prepare for an asset inventory, a baseline of the asset account will be produced by the ECO and provided to the PC. **(T-1).**

A3.3.1.1. ECO will generate an inventory list in DPAS based on the inventory type (Custodian, Cyclic by Custodian, Cyclic by Location, Location, Sensitive, and Custom) and provide the report to the responsible PC. **(T-1).**

A3.3.2. To assist in this process, the account owner can use a combination of asset discovery/automated inventory tools and manual identification of assets.

A3.3.2.1. The account owner can utilize enterprise asset discovery tools to perform a network scan to “discover” assets on the network that are within their account.

A3.3.3. this discovery cannot be done any earlier than one month prior to the inventory due date.

A3.3.4. One month of scanning will produce a list of assets that have been on the network at various times over that scanning period and this list may be included as a component of the inventory of a complete account.

A3.4. Performing the Inventory. To perform an asset inventory, the PC will:

A3.4.1. Ensure that all assets in their account(s) have been identified. **(T-1).**

A3.4.2. Ensure that gains/losses against the inventory baseline are documented and reconciled. **(T-1).**

A3.4.3. If using Automated Inventory Tool (AIT), the physical inventory can be performed only on those assets not identified using the AIT.

A3.5. Completing the Inventory. To complete an asset inventory, the UAPO will:

A3.5.1. Ensure that the individual performing the inventory has signed, indicating that the inventory is complete and accurate. **(T-1).**

A3.5.2. Endorse the signed inventory with signature, accepting responsibility for the results. **(T-1).**

A3.5.3. Will provide the completed, signed, and endorsed inventory in an electronic format to the installation ECO for record. **(T-1).**

A3.5.4. Upon signature, PA will upload signed documentation to DPAS and update the date of last inventory for all assets within the account. **(T-1).**

A3.6. Finalizing the Inventory. To finalize an asset inventory, the ECO will reconcile all gain/loss annotations in DPAS. **(T-1).**

A3.7. Random Sampling. AFECO will perform random sampling of IT asset enterprise to ensure inventory requirements are being adhered to. **(T-1).**

ATTACHMENT 4

IT HARDWARE KEY SUPPORTING DOCUMENTS (KSDs) AND MANDATORY DATA ELEMENTS

A4.1. Purpose and Scope. The intent of this plan is to articulate the minimum requirements for creating and maintaining KSDs for IT hardware assets. Additional requirements that may be levied onto units by their parent MAJCOM/DRU/FOA organization will be articulated in a MAJCOM/DRU/FOA-specific plan.

A4.2. IT Asset Life Cycle. KSDs will be retained throughout the following phases of the asset life cycle:

A4.2.1. Plan. This phase includes activities in which the asset requirement is generated and approved. **(T-1).**

A4.2.2. Acquisition. This phase includes activities in which the asset order is generated and approved, funds are executed, and the asset is shipped to the customer. **(T-1).**

A4.2.3. Fielding. This phase includes activities in which the asset arrives at the warehouse, entered into the DPAS, staged for fielding, and fielded. **(T-1).**

A4.2.4. Management. This phase includes activities in which the asset is inventoried, transferred, and updated. **(T-1).**

A4.2.5. Retirement. This phase includes activities in which asset disposition is requested, staged for disposition, sent to DRMS/DLADS, and updated in DPAS. **(T-1).**

A4.3. Retaining KSDs

A4.3.1. All KSDs must be uploaded in DPAS as an attachment to the pertinent asset record and retained in accordance with AFI 33-322. **(T-1).**

A4.3.1.1. DPAS will serve as the primary records management system, but UAPOs and ECOs may determine and follow additional local procedures. **(T-1).**

Table A4.1. Key Supporting Documents (KSDs) Requirements.

Below table outlines requirements for which transactions must include a KSD, minimum data requirements for each KSD, and responsible parties.

Life Cycle Transaction	Key Supporting Document (KSD)	Retention	Mandatory Data Elements	Acceptable Range of Documents	Responsible Entity
Requirement generated	In accordance with local process	Conditional	In accordance with local process	In accordance with local process	PC
Requirement approved	In accordance with local process	Conditional	In accordance with local Process	In accordance with local process	PC
Order generated	Web based activity	Conditional	In accordance with local process	In accordance with local process	PC
Order approved	Web based activity	Conditional	In accordance with local process	In accordance with local process	PC and ECO
Funds executed, shipped to customer	Web based activity	Conditional	In accordance with local process	In accordance with local process	Vendor
Arrives at warehouse	Document	Mandatory	Date, price, serial, part, manufacturer CAGE	Shipping invoice, bill of lading, contract, receipt, MFR	Vendor
Asset record created in DPAS	DPAS transaction	Mandatory	Date, price, serial, part, manufacturer CAGE	DPAS transaction	ECO
Staged for fielding	DPAS transaction	Conditional	Old location, new location	DPAS transaction	ECO
Fielded	DPAS transaction	Mandatory	Old location, new location	DPAS transaction	ECO
Inventory	DPAS transaction	Mandatory	Date of last inventory (DOLI)	DPAS transaction /document	PC
Transfer	DPAS transaction	Conditional	Old location, new location	DPAS transaction, DD form 1149	PC and ECO
Location updated	DPAS transaction/document	Conditional	Old location, new location	DPAS transaction /Document	PC and ECO
Disposition requested	DPAS transaction	Mandatory	DPAS transaction	DPAS transaction	PC and ECO
Serviceable asset advertised	Web based activity	Conditional	Conditional	Conditional	ECO
Staged for disposition	DPAS transaction/document	Conditional	Conditional	Conditional	PC and ECO
Sent to DRMS/DLADS	DPAS transaction/document	Mandatory	Date, price, serial, part, manufacturer CAGE	DD form 1348-1A, ETIDs, MFR	PC and ECO
Asset updated in DPAS	DPAS transaction/Document	Mandatory	Date, price, serial, part, CAGE	DD form 1348-1A, ETIDs, MFR	PC and ECO

ATTACHMENT 5
Examples of IUS and Non-IUS.

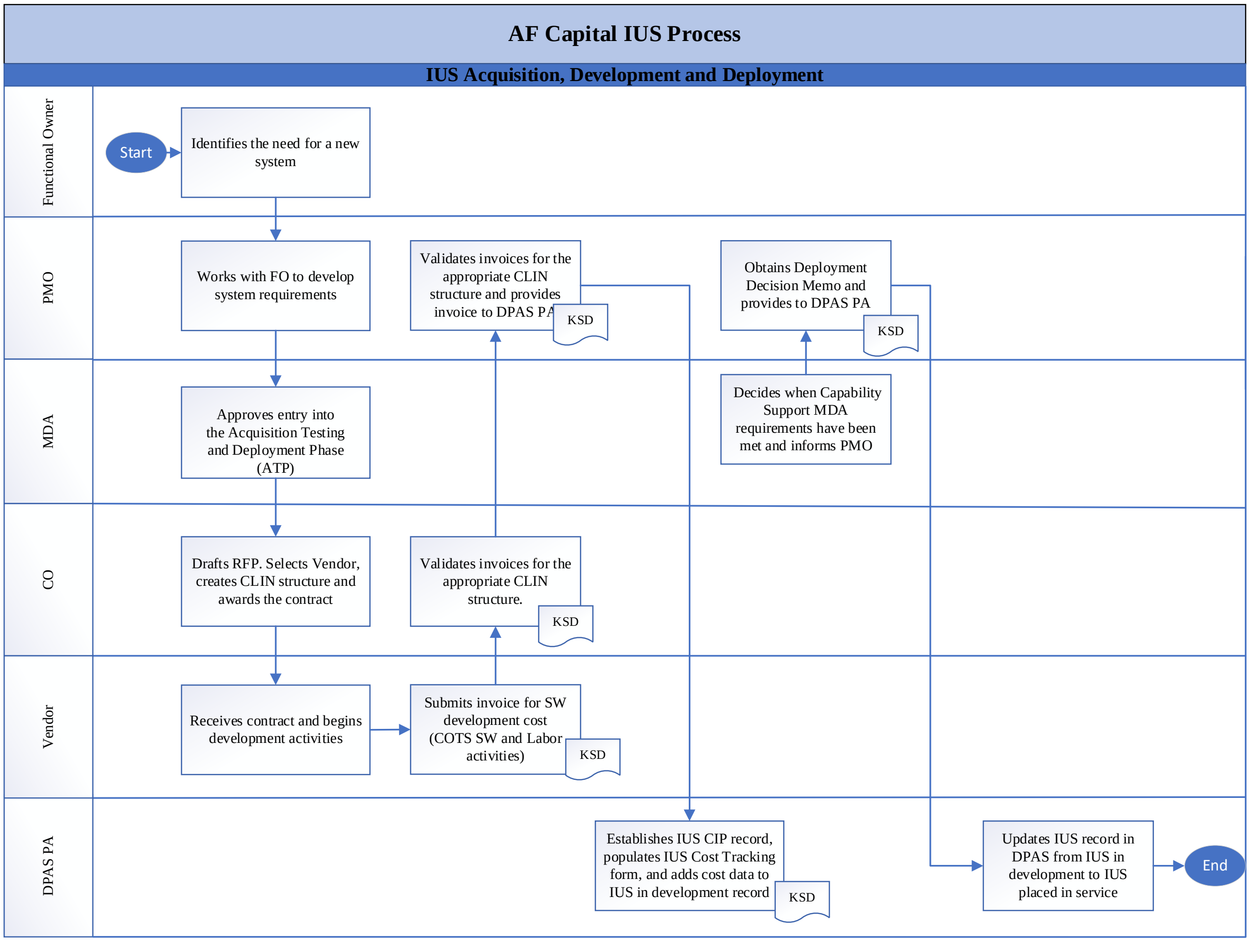
Definition	IUS		Examples
Access Control Software			
This type of software, which is external to the operating system, provides a means of specifying who has access to a system and the specific capabilities authorized users are granted.	NO		Common Access Card (CAC) Reader Software
Application Software			
A software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.	YES		Microsoft (MS) Excel, Adobe Photoshop, MS Project, MS Visio
Cloud, Public Infrastructure			
A cloud-based environment that is generally external to the Air Force with infrastructure owned and managed by a third party. Public cloud services are generally subscription based.	NO		Amazon Web Services (AWS), Azure
Cloud, Private			
An on-premises cloud-based environment that is generally internal to the Air Force and used solely by the Air Force.	YES		Army Private Cloud Enterprise (APCE), Redstone
Database Management Systems			
Commercial software that integrates business information flowing through the Component. Enterprise Resource Planning (ERP) systems contain functional modules (e.g., financial, accounting, human resources, supply chain, and customer information) that are integrated within the core system or interfaced to external systems.	YES		Oracle
Enterprise Resource Planning System			
Commercial software that integrates business information flowing through contain functional modules (e.g., financial, accounting, human resources, supply chain, and customer information) that are integrated within the core system or interfaced to external systems.	YES		Defense Enterprise Accounting and Management System (DEAMS)
Firmware			
A program recorded in permanent or semi-permanent computer memory. Firmware should be capitalized as part of equipment it is integrated into.	NO		Radar system software, lathe software
Freeware/Open Source Software			
Software that is offered at no cost.	NO		Internet Explorer (IE), Chrome, Firefox,
Software Integrated into Hardware			
Software that is integrated into the physical components of IT, including into servers, computers, peripheral devices, disks, scanners, switches, and other IT equipment.	NO		Computer Operating Systems
Software License – Annual			
A software license that must be renewed annually to continue using the software (with the expectation that the Air Force will renew the license).	YES		MS Lync, VMWare, vSphere

Definition	IUS		Examples
Software License – Enterprise			
A license that allows use of the software throughout an organization or for a specified number of users.	YES		MS Office, Oracle
Software License – Perpetual			
A software license that gives the Air Force the right to use the software in perpetuity.	YES		Systems, Applications and Products (SAP)
Middleware			
Computer software that provides services to software applications beyond those available from the operating system.	YES		Air Force system to system interfaces
Portal			
Web-based application that provides personalization, single sign-on, and content aggregation from different sources, and hosts the presentation layer of information systems.	YES		Air Force Portal, Customized Microsoft (MS) SharePoint Sites
Simulation Software			
Based on the process of modeling a real or proposed system with a set of mathematical formulas that allows the user to observe an operation before performing it.	NO		Flight Training Software
Operating System			
The software that controls the execution of other computer programs, schedules tasks, allocates storage, manages the interface to peripheral hardware, and presents a default interface to the user when no application program is running.	NO		Windows, Linux, iOS
System/IT System			
The term "system" by itself is not limited to any specific resource. A system may be any two resources that work together to produce a specific outcome. IUS may or may not be one component of an overall "system".	YES		IT Investment Portfolio System (ITIPS), Defense Enterprise Accounting and Management System (DEAMS)
Utility Program			
System software designed to perform a particular function or system maintenance.	NO		Burner, calculator, virus scan
Web Application			
An application that is accessed via the web over a network.	YES		Webmail
Audio/Visual Equipment			
Audio and Visual equipment have generally integrated software which is not IUS.	NO		VTC, CISCO phone equipment
Outsourced IT			
Software capabilities provided by non-Air Force entities and using COTS IUS licenses owned by those non-Air Force entities.	NO		Cloud services
Software as a Service (SaaS)			
Any COTS IUS license provided to DOD users as a service, which may be identified as cloud computing, software as a service, or other “as a service” software subscriptions are not accounted as IUS.	NO		Microsoft 365

Definition	IUS		Examples
Network			
Normally network consists of routers and switches which utilizes integrated software and do not qualify as IUS. If the member’s investment has been identified as network and does not have software components such as Network Operations (NETOPS) tools (e.g., Microsoft System Center Configuration Manager (SCCM), Tanium ®, Host Based Security System (HBSS)) then it is not an IUS.	NO		Secret Internet Protocol (IP) Router Network (SIPRNet), Non-classified Internet Protocol (IP) Router Network (NIPRNet)
Exception: If network has additional software other than those integrated into switches and routers, then it is considered an IUS and be accountable as such.	YES		Microsoft System Center Configuration Manager (SCCM), Host Based Security System (HBSS), Tanium ®, SolarWinds ®
Weapon System (Military Equipment)			
In accordance with DOD FMR 7000.14-R, Chapter 25, section 250201, IUS (Account 1830); “*Intangible items, such as software, are not considered weapon systems; however, computer software that is integrated into (embedded) and necessary to operate weapon systems (rather than perform an application) must be considered part of the weapon system of which it is an integral part*”.	NO		Air Force weapons and weapon systems
Exception: Information systems supporting weapons systems will be accounted as IUS.	YES		Air Force weapons system

ATTACHMENT 6

Figure 6.1. Developed IUS Acquisition, Development and Deployment Process.


AF Capital IUS Process
IUS Acquisition, Development and Deployment
Functional Owner
PMO
MDA
CO
Vendor
DPAS PA
Start
Identifies the need for a new system
Works with FO to develop system requirements
Validates invoices for the appropriate CLIN structure and provides invoice to DPAS PA
KSD
Obtains Deployment Decision Memo and provides to DPAS PA
KSD
Approves entry into the Acquisition Testing and Deployment Phase (ATP)
Decides when Capability Support MDA requirements have been met and informs PMO
Drafts RFP. Selects Vendor, creates CLIN structure and awards the contract
Validates invoices for the appropriate CLIN structure.
KSD
Receives contract and begins development activities
Submits invoice for SW development cost (COTS SW and Labor activities)
KSD
Establishes IUS CIP record, populates IUS Cost Tracking form, and adds cost data to IUS in development record
KSD
Updates IUS record in DPAS from IUS in development to IUS placed in service
End

ATTACHMENT 7

Figure 7.1. Enterprise Software Acquisition and Deployment Process.

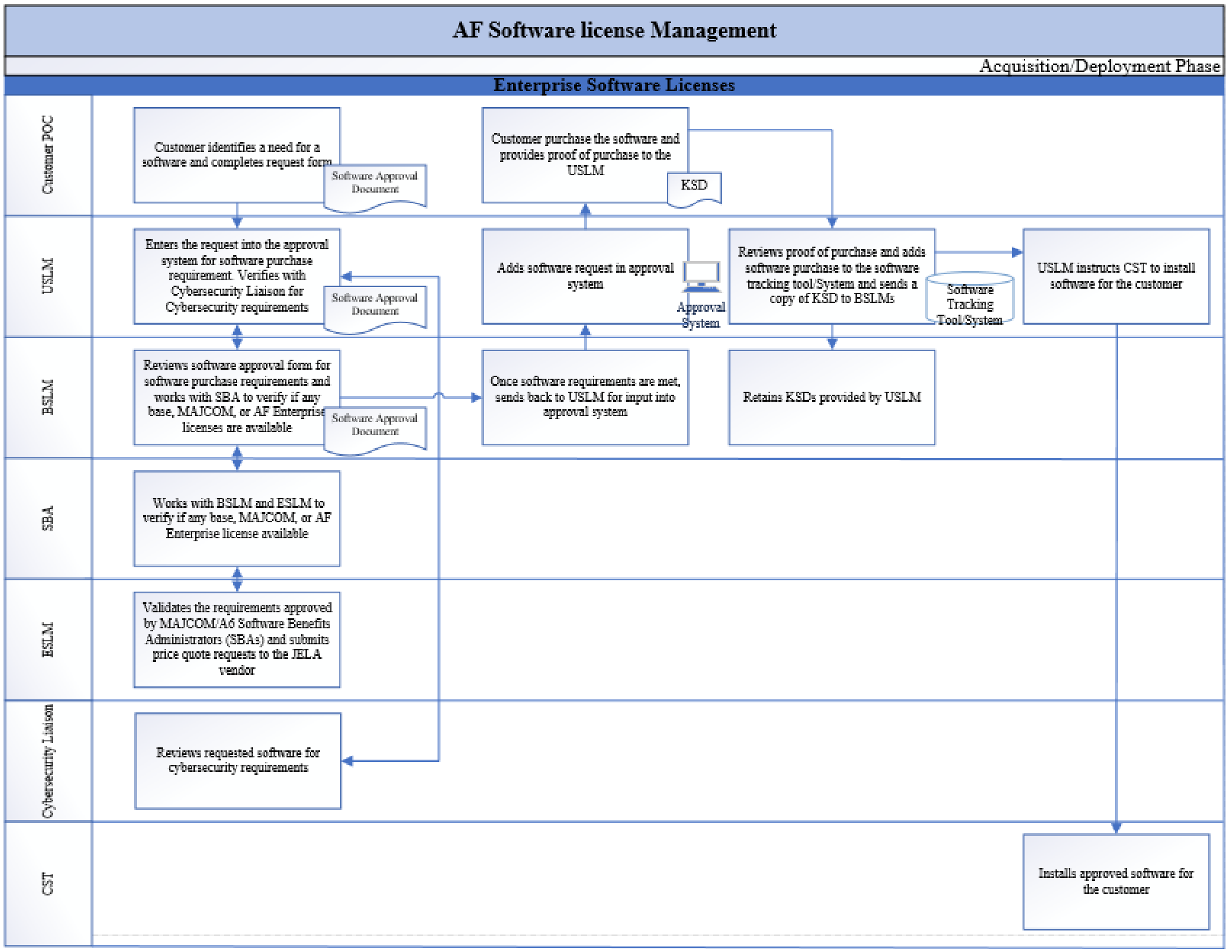

AF Software license Management
Acquisition/Deployment Phase
Enterprise Software Licenses
Customer POC
USLM
BSLM
SBA
ESLM
Cybersecurity Liaison
CST
Customer identifies a need for a software and completes request form
Software Approval Document
Customer purchase the software and provides proof of purchase to the USLM
KSD
Enters the request into the approval system for software purchase requirement. Verifies with Cybersecurity Liaison for Cybersecurity requirements
Software Approval Document
Adds software request in approval system
Approval System
Reviews proof of purchase and adds software purchase to the software tracking tool/System and sends a copy of KSD to BSLMs
Software Tracking Tool/System
USLM instructs CST to install software for the customer
Reviews software approval form for software purchase requirements and works with SBA to verify if any base, MAJCOM, or AF Enterprise licenses are available
Software Approval Document
Once software requirements are met, sends back to USLM for input into approval system
Retains KSDs provided by USLM
Works with BSLM and ESLM to verify if any base, MAJCOM, or AF Enterprise license available
Validates the requirements approved by MAJCOM/A6 Software Benefits Administrators (SBAs) and submits price quote requests to the JELA vendor
Reviews requested software for cybersecurity requirements
Installs approved software for the customer

Figure 7.2. Non-Enterprise Software Acquisition and Deployment Process.

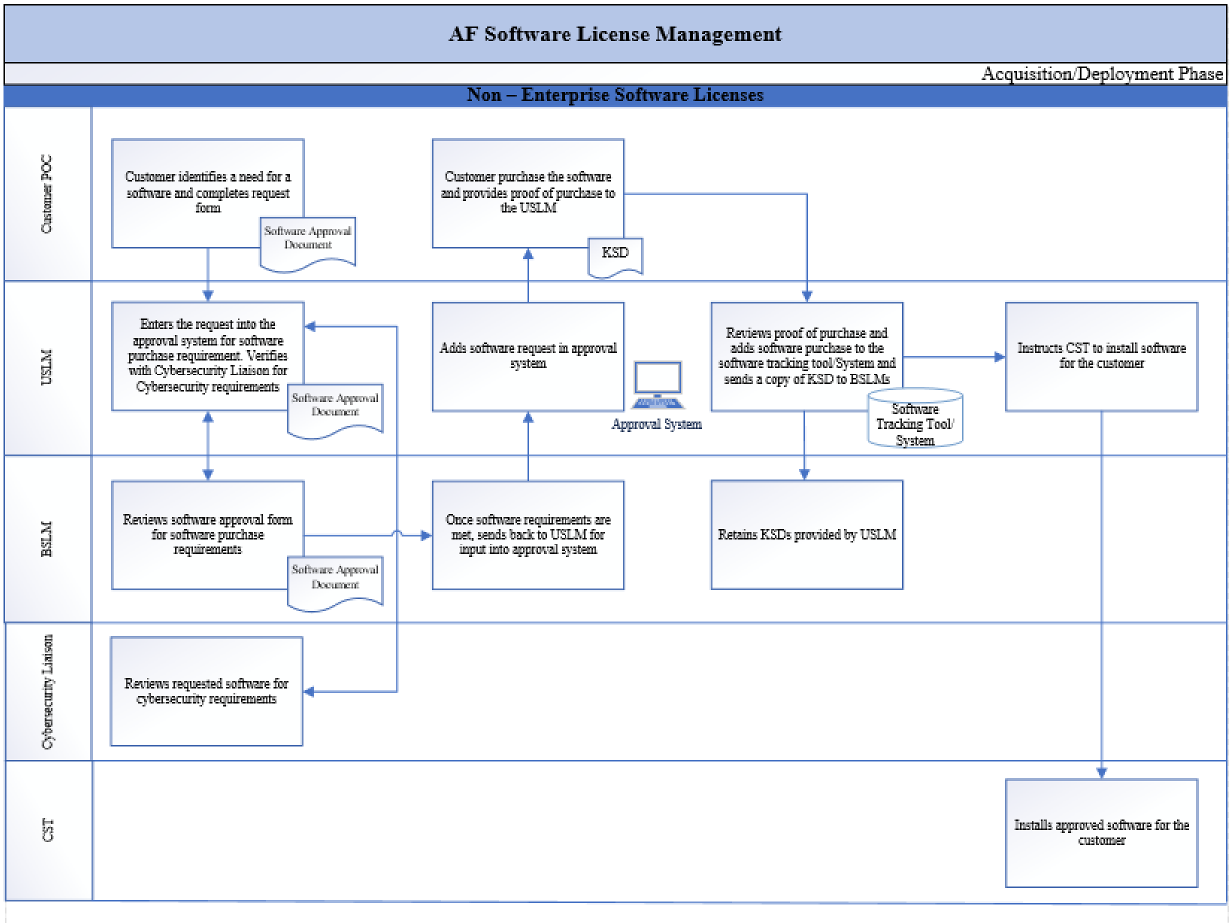
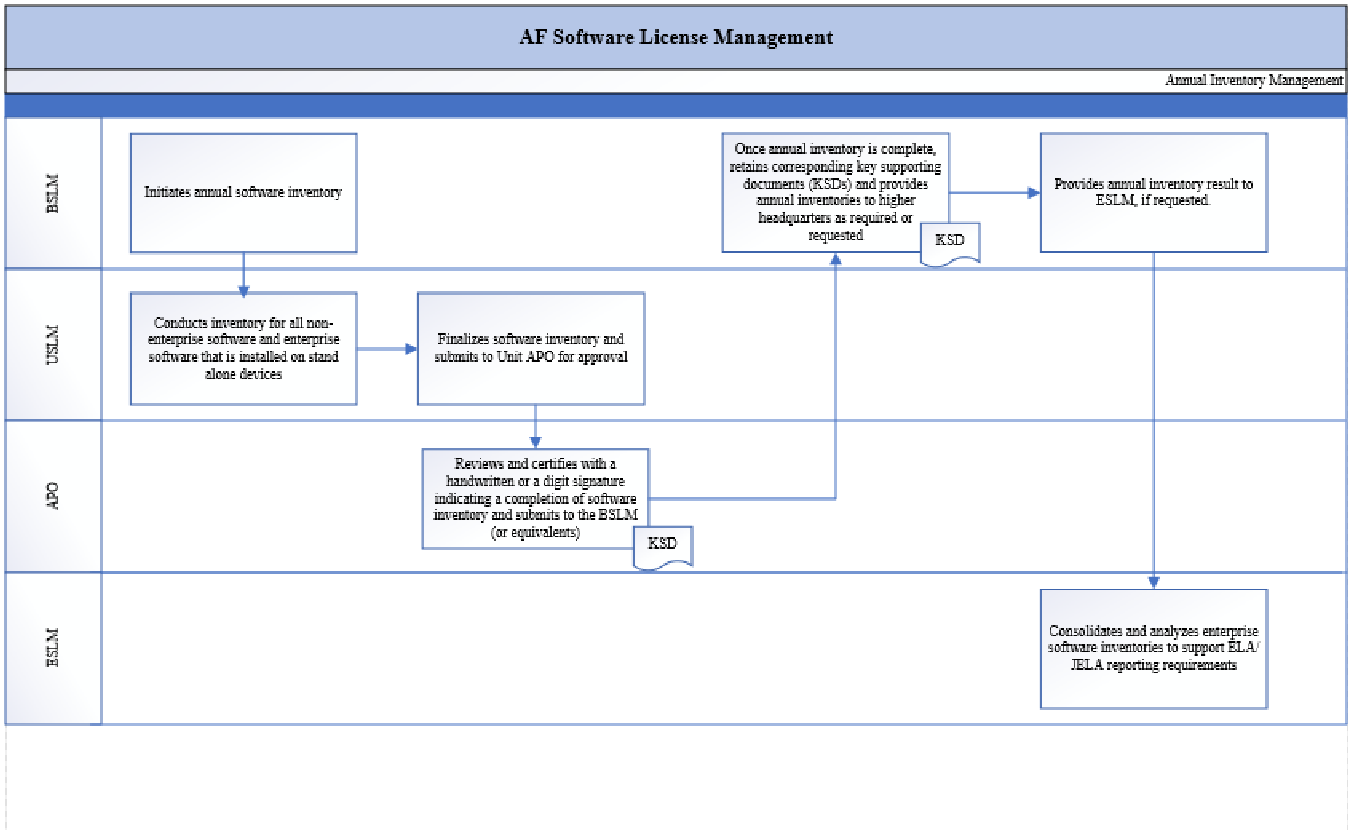
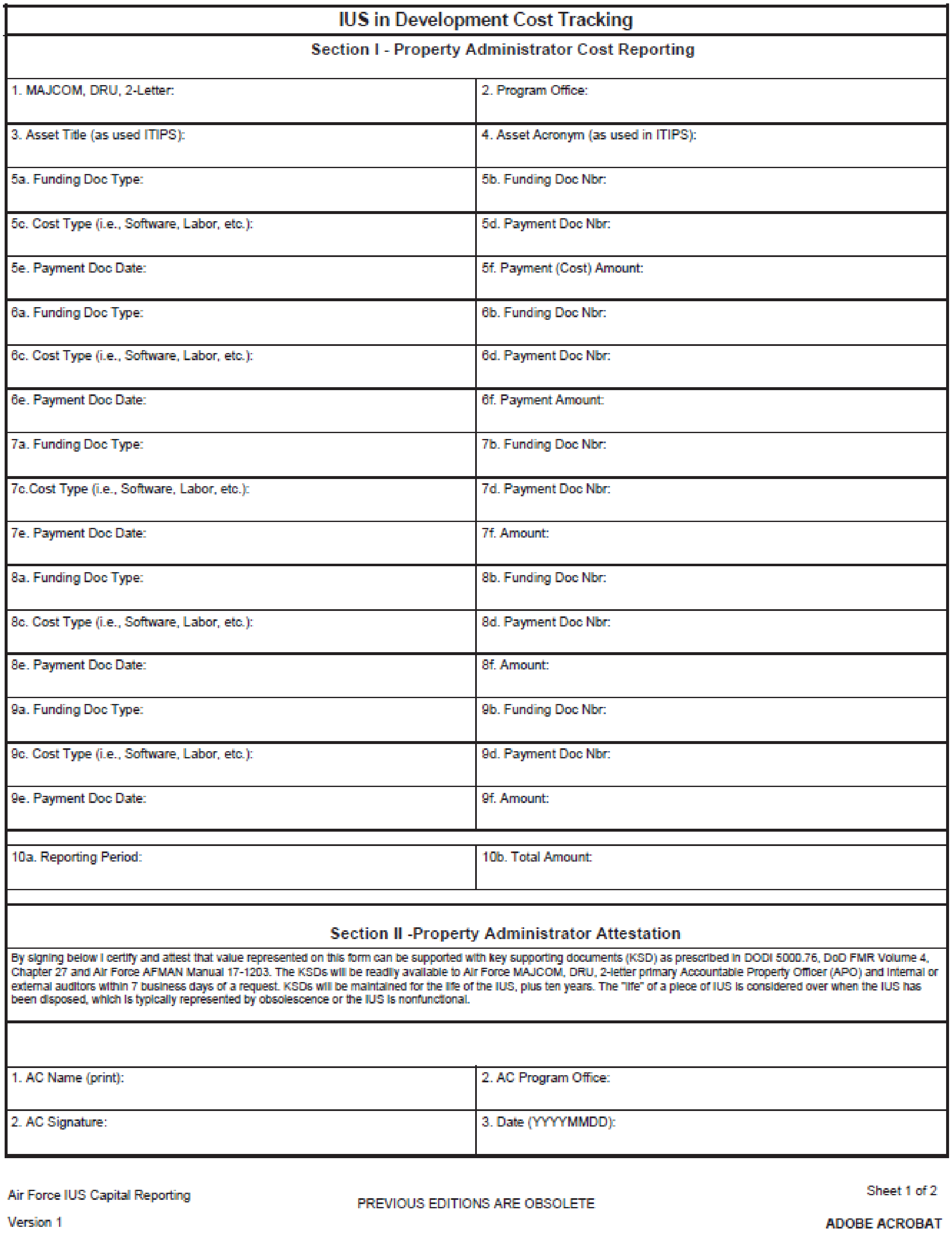

AF Software License Management
Acquisition/Deployment Phase
Non – Enterprise Software Licenses
Customer POC
USLM
BSLM
Cybersecurity Liaison
CST
Customer identifies a need for a software and completes request form
Software Approval Document
Customer purchase the software and provides proof of purchase to the USLM
KSD
Enters the request into the approval system for software purchase requirement. Verifies with Cybersecurity Liaison for Cybersecurity requirements
Software Approval Document
Adds software request in approval system
Approval System
Reviews proof of purchase and adds software purchase to the software tracking tool/System and sends a copy of KSD to BSLMs
Software Tracking Tool/ System
Instructs CST to install software for the customer
Reviews software approval form for software purchase requirements
Software Approval Document
Once software requirements are met, sends back to USLM for input into approval system
Retains KSDs provided by USLM
Reviews requested software for cybersecurity requirements
Installs approved software for the customer

Figure 7.3. Software Annual Inventory Process.


AF Software License Management
Annual Inventory Management
BSLM
USLM
APO
ESLM
Initiates annual software inventory
Conducts inventory for all non-enterprise software and enterprise software that is installed on stand alone devices
Finalizes software inventory and submits to Unit APO for approval
Reviews and certifies with a handwritten or a digit signature indicating a completion of software inventory and submits to the BSLM (or equivalents)
KSD
Once annual inventory is complete, retains corresponding key supporting documents (KSDs) and provides annual inventories to higher headquarters as required or requested
KSD
Provides annual inventory result to ESLM, if requested.
Consolidates and analyzes enterprise software inventories to support ELA/ JELA reporting requirements

ATTACHMENT 8

Air Force Form 7500, Internal Use Software Cost Tracking



IUS in Development Cost Tracking

Section I - Property Administrator Cost Reporting

1. MAJCOM, DRU, 2-Letter:	2. Program Office:
3. Asset Title (as used ITIPS):	4. Asset Acronym (as used in ITIPS):
5a. Funding Doc Type:	5b. Funding Doc Nbr:
5c. Cost Type (i.e., Software, Labor, etc.):	5d. Payment Doc Nbr:
5e. Payment Doc Date:	5f. Payment (Cost) Amount:
6a. Funding Doc Type:	6b. Funding Doc Nbr:
6c. Cost Type (i.e., Software, Labor, etc.):	6d. Payment Doc Nbr:
6e. Payment Doc Date:	6f. Payment Amount:
7a. Funding Doc Type:	7b. Funding Doc Nbr:
7c.Cost Type (i.e., Software, Labor, etc.):	7d. Payment Doc Nbr:
7e. Payment Doc Date:	7f. Amount:
8a. Funding Doc Type:	8b. Funding Doc Nbr:
8c. Cost Type (i.e., Software, Labor, etc.):	8d. Payment Doc Nbr:
8e. Payment Doc Date:	8f. Amount:
9a. Funding Doc Type:	9b. Funding Doc Nbr:
9c. Cost Type (i.e., Software, Labor, etc.):	9d. Payment Doc Nbr:
9e. Payment Doc Date:	9f. Amount:
10a. Reporting Period:	10b. Total Amount:

Section II -Property Administrator Attestation

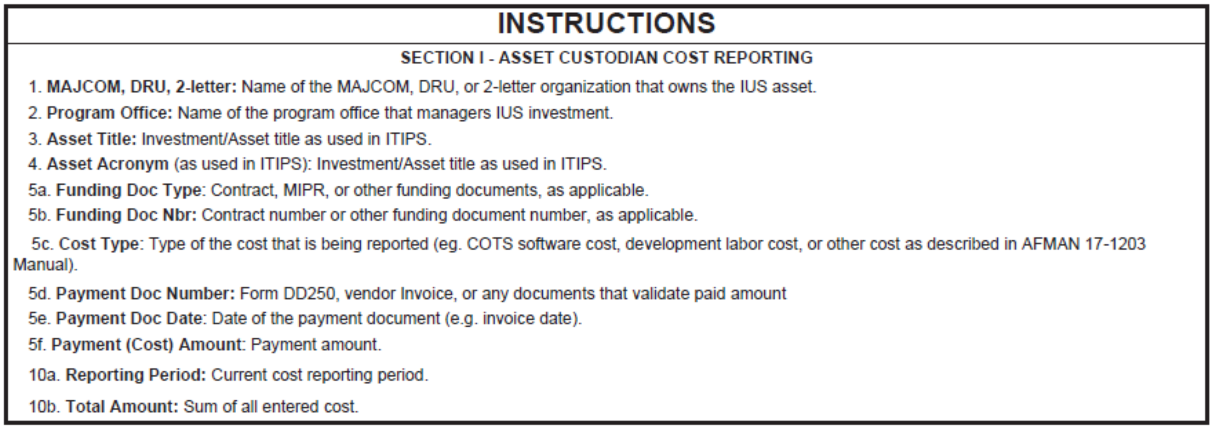
By signing below I certify and attest that value represented on this form can be supported with key supporting documents (KSD) as prescribed in DODI 5000.76, DoD FMR Volume 4, Chapter 27 and Air Force AFMAN Manual 17-1203. The KSDs will be readily available to Air Force MAJCOM, DRU, 2-letter primary Accountable Property Officer (APO) and internal or external auditors within 7 business days of a request. KSDs will be maintained for the life of the IUS, plus ten years. The "life" of a piece of IUS is considered over when the IUS has been disposed, which is typically represented by obsolescence or the IUS is nonfunctional.

1. AC Name (print):	2. AC Program Office:
2. AC Signature:	3. Date (YYYYMMDD):

Air Force IUS Capital Reporting
Version 1

PREVIOUS EDITIONS ARE OBSOLETE

Sheet 1 of 2
ADOBE ACROBAT



INSTRUCTIONS

SECTION I - ASSET CUSTODIAN COST REPORTING

1. **MAJCOM, DRU, 2-letter:** Name of the MAJCOM, DRU, or 2-letter organization that owns the IUS asset.

2. **Program Office:** Name of the program office that managers IUS investment.

3. **Asset Title:** Investment/Asset title as used in ITIPS.

4. **Asset Acronym** (as used in ITIPS): Investment/Asset title as used in ITIPS.

5a. **Funding Doc Type**: Contract, MIPR, or other funding documents, as applicable.

5b. **Funding Doc Nbr:** Contract number or other funding document number, as applicable.

5c. **Cost Type**: Type of the cost that is being reported (eg. COTS software cost, development labor cost, or other cost as described in AFMAN 17-1203 Manual).

5d. **Payment Doc Number:** Form DD250, vendor Invoice, or any documents that validate paid amount

5e. **Payment Doc Date**: Date of the payment document (e.g. invoice date).

5f. **Payment (Cost) Amount**: Payment amount.

10a. **Reporting Period:** Current cost reporting period.

10b. **Total Amount:** Sum of all entered cost.

BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 17-1203

18 MAY 2018

Communications and Information

INFORMATION TECHNOLOGY (IT) ASSET MANAGEMENT (ITAM)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/CIO A6SE

Certified by: SAF/CIO A6S
(Col Michael S. Strunk)

Supersedes: AFMAN17-1203, 19 March 2014

Pages: 36

This Air Force Manual (AFMAN) implements Executive Order (E.O.) 13103, *Computer Software Piracy and Air Force Policy Directives* (AFPD) 17-1, *Information Dominance Governance and Management* and supports AFPD 17-2, *Cyberspace Operations*, and AFPD 10-6, *Capabilities Requirements Development*. This AFMAN provides the overarching guidance and direction for managing IT hardware and software. The hardware management guidance identifies responsibilities for supporting Air Force (AF) IT hardware (IT assets). The software management guidance identifies responsibilities for management of commercial off-the-shelf (COTS) software. This AFMAN applies to the Air National Guard (ANG) and the Air Force Reserve (AFR) unless indicated otherwise. One or more paragraphs of this AFMAN may not apply to non-AF-managed joint service systems. These paragraphs are marked as follows: (NOT APPLICABLE TO NON-AF-MANAGED JOINT SERVICE SYSTEMS). The authorities to waive wing/unit level requirements in this publication are identified with a Tier (“T-0, T-1, T-2, and T-3”) number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, Table 1.1., for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or for non-tiered compliance items, the local commander. Send recommended changes or comments, through appropriate command channels, to Enterprise IT Integration Division (SAF/CIO A6SE) using AF Form 847, *Recommendation for Change of Publication*. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. See Attachment 1 for a glossary of references and supporting information.

SUMMARY OF CHANGES

This document has been substantially revised and needs to be completely reviewed. Major changes include adjustment to the Roles and Responsibilities, inclusion of the Host Commander as responsible for appointing a Host Accountable Property Officer (APO), removal of the Property Custodian and Client Systems Administrator roles, adjustment to accountability determination for Information Technology (IT), removal of guidance addressed in other publications, removal of specific verbiage related to acquisition of IT hardware and software, an update to software policy to include Internal Use Software (IUS), and the deletion of Chapter 4, NETCENTS-2.

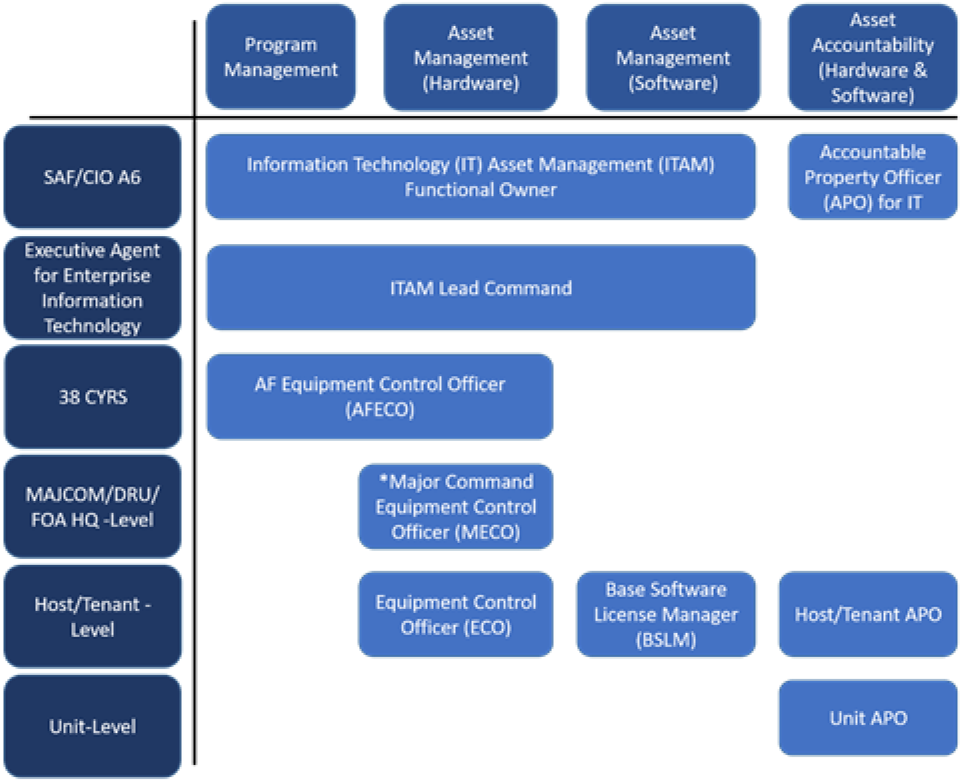
Chapter 1

IT ASSET MANAGEMENT

1.1. Overview. This manual provides guidance and direction for operational management of IT hardware and software. Hardware management guidance identifies responsibilities for supporting AF IT hardware assets including maintaining physical accountability of Personal Wireless Communications Systems (PWCS). Refer to AFI 17-210, Radio Management, for overall PWCS management guidance. Software management guidance identifies responsibilities for operational management of COTS and AF-unique software acquired or developed by the AF (other than software internal to a weapon system). Refer to AFI 63-101/20-101, Integrated Life Cycle Management, for guidelines, policies, and procedures for AF personnel who develop, review, approve, or manage systems, subsystems, end-items, and services. Technologies and techniques for continuous network monitoring and automatic tracking of hardware and software assets will be used to the maximum extent possible in place of manual physical inventories. Manual inventories and procedures must continue to be followed for hardware or software that cannot be accounted for with automated tracking techniques due to assets not installed, not configurable as discoverable, or not connected to a monitored network, (T-1).

1.2. Roles and Responsibilities. **Figure 1.1** below represents an overview of those Information Technology Asset Management (ITAM) roles and responsibilities from the AF to the organizational level.

Figure 1.1. Information Technology Asset Management Roles and Responsibilities Overview.



	Program Management	Asset Management (Hardware)	Asset Management (Software)	Asset Accountability (Hardware & Software)
SAF/CIO A6	Information Technology (IT) Asset Management (ITAM) Functional Owner			Accountable Property Officer (APO) for IT
Executive Agent for Enterprise Information Technology	ITAM Lead Command			
38 CYRS	AF Equipment Control Officer (AFECO)			
MAJCOM/DRU/ FOA HQ -Level		*Major Command Equipment Control Officer (MECO)		
Host/Tenant - Level		Equipment Control Officer (ECO)	Base Software License Manager (BSLM)	Host/Tenant APO
Unit-Level				Unit APO

* = may not reside at the MAJCOM/DRU/FOA HQ

1.2.1. **Secretary of the Air Force, Chief, Information Dominance & Chief Information Officer (SAF/CIO A6).**

1.2.1.1. Develops strategy, policy, and guidance for Information Technology (IT) Asset Management (ITAM) of IT hardware and software.

1.2.1.2. Resolves management issues and policy disagreements between Major Commands (MAJCOMs), functional managers, and non-AF agencies for IT hardware and software assets.

1.2.1.3. Identifies, reviews, approves, and forwards formal ITAM training requirements to Headquarters Air Education and Training Command.

1.2.1.4. As the Functional Manager, designates the Accountable Property System of Record (APSR) to support ITAM accountability according to Attachment 2.

1.2.1.5. Ensures primary Accountable Property Officers (APO) are appointed as needed.

1.2.1.6. Requires APOs to be appointed in writing at appropriate level.

1.2.1.7. Surveys, consolidates, validates, and tracks all MAJCOM, Field Operating Agency (FOA), and Direct Reporting Unit (DRU) requirements for potential AF enterprise software licenses for COTS software.

1.2.1.8. Recommends candidate software products for potential AF-wide or Department of Defense (DoD)-wide licensing to the Air Force Materiel Command (AFMC) product center designated with the responsibility for procurement of enterprise licenses as the purchasing agent.

1.2.1.9. Serves as the AF software license manager to review and consolidate the AF software license inventory in coordination with the Executive Agent for Enterprise Information Technology. MAJCOM and base inventories include locally-owned software and software not yet transferred to an enterprise software license agreement.

1.2.1.10. In coordination with AFMC, designates a product center as the Office of Primary Responsibility (OPR) for managing the AF Enterprise Software License Program and, when designated, acts as executive agent for establishing DoD-wide enterprise software license agreements.

1.2.1.11. Ensures warfighting systems software compliance with Department of Defense Instruction (DoDI) 8320.02, *Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense,* (T-0).

1.2.2. **Director, Security, Counterintelligence, and Special Program Oversight (SAF/AAZ).**

1.2.2.1. Special Access Programs (SAP) Information Technology (IT) hardware assets will be tracked in the designated APSR or another approved APSR. The Director will evaluate all security issues and concerns and render a determination in writing as to which assets will be tracked.

1.2.2.2. IT hardware assets which cannot be tracked using an approved APSR will be tracked separately within the SAP configuration control project databases, (T-0).

1.2.3. **Deputy Chief of Staff, Intelligence, Surveillance, and Reconnaissance, (AF/A2).**

1.2.3.1. The AF/A2 is the AF Lead for systems in AF Sensitive Compartmented Information Facilities (SCIFs), AF Sensitive Compartmented Information (SCI) systems, and national-level intelligence, surveillance and reconnaissance systems IAW DoDI 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)*, AFPD 17-2, *Cyberspace Operations*, and AFI 17-130, *Cybersecurity Program Management*.

1.2.3.2. AF IT hardware assets under the control of AF/A2 will be tracked in the designated Accountable Property System of Record (APSR), or other approved accountable systems of record for accountability of hardware, (T-0). The designated security authority representative will evaluate all security issues and concerns before rendering a determination as to where and which assets will be tracked. AF/A2 or designated representative will provide guidance for meeting regulatory compliance for IT hardware assets not tracked in the designated APSR.

1.2.4. **Executive Agent for Enterprise Information Technology:**

1.2.4.1. Serves as lead for implementation of Information Technology Asset Management (ITAM).

1.2.4.2. Publishes software entitlements, implementation and ITAM account inventory metrics.

1.2.4.3. Manages the AF Evaluated Products List (AF EPL) and publishes to the AF Portal the certified COTS Software Products for use on AF networks.

1.2.4.4. Coordinates with SAF/CIO A6, AFMC and MAJCOMs for software license requirements and consolidates non-enterprise software agreements.

1.2.4.5. Identifies and forwards formal ITAM training requirements to SAF/CIO A6.

1.2.5. **Air Force Equipment Control Officer (AFECO):**

1.2.5.1. The 38th Cyberspace Readiness Squadron (38 CYRS) serves as the AFECO for all AF IT hardware assets within the designated APSR.

1.2.5.2. Provides guidance and support to MAJCOMs, FOAs, and DRUs in managing Information Technology (IT) hardware assets.

1.2.5.3. Reviews, evaluates, and interprets issues and problems as the ITAM subject matter expert and makes recommendations on ITAM policy changes to SAF/CIO A6.

1.2.5.4. Coordinates with SAF/CIO A6 to propose changes, upgrades, and/or modifications to the designated APSR.

1.2.5.4.1. Manages the designated APSR accounts for ECOs, to include approving new account requests.

1.2.5.5. Approves appointment of Major Command Equipment Control Officers (MECOs) and performs responsibilities described in this AFMAN as required by MAJCOM Memorandum of Agreements (MOA) governing the transfer of A6 workload responsibilities to Executive Agent for Enterprise Information Technology.

1.2.5.5.1. Maintains the list of designated MECOs and Equipment Control Officers (ECOs).

1.2.5.6. Manages the implementation of DoD and AF policy on Serialized Item Management (SIM) and Item Unique Identification (IUID) according to AFI 63-101/20-101, *Integrated Life Cycle Management*, for all IT hardware assets managed in the designated Accountable Property System of Record (APSR) as applicable.

1.2.5.7. Monitors appointment of APOs and notifies SAF/CIO A6 of required appointments.

1.2.5.8. Has authority to freeze a Primary Asset Account for failure to comply with requirements described in this manual.

1.2.6. **Air Force Materiel Command (AFMC)** :

1.2.6.1. Designates a product center as purchasing agent for software licenses to support consolidated and programmatic AF requirements.

1.2.6.2. Designates the Managed Services Office (MSO) for managing the commoditized purchase of AF infrastructure and platform service components. The Managed Services Office (MSO) establishes AF enterprise commoditized purchase and provisioning of infrastructure ensuring the management of IT assets within the infrastructure.

1.2.7. **Air Education and Training Command (AETC):**

1.2.7.1. Supports and develops Information Technology Asset Management (ITAM) training plans and materials.

1.2.8. **MAJCOM, DRU, FOA, or Equivalent:**

1.2.8.1. Appoints a Major Command Equipment Control Officer (MECO), when this role is not designated by a previous MOA, documents acknowledgement of duties with handwritten or digital signatures, and provides a copy to the AFECO, (T-1).

1.2.8.2. Notifies 38 CYRS/SCM via email at **AFECO@us.af.mil** when the MECO changes.

1.2.8.3. Ensures all commercial off-the-shelf (COTS) license requirements are purchased using approved DoD/AF Enterprise Licenses Agreements (ELAs), DoD ESI or approved DoD/AF contract vehicles, (T-1).

1.2.9. **Major Command Equipment Control Officer (MECO).** The MECO will:

1.2.9.1. Serve as the Command liaison between the AFECO and ECO.

1.2.9.1.1. Not be the ECO in the same command according to DoD *Financial Management Regulation* (DoDFMR) 7000.14-R, Volume 3, Chapter 8, *Federal Financial Management Improvement Act Compliance* and AFI 65-201, *Managers' Internal Control Program Procedures*, (T-0).

1.2.9.2. Maintain the list of designated ECOs.

1.2.9.3. Ensure compliance with this AFMAN across their portfolio.

1.2.9.4. Resolve compliance issues when resolution is unable to be performed at the Host/Tenant APO level.

1.2.9.5. Provide reports to Host APO, MAJCOM A6 or MAJCOM Inspection Teams, upon request.

1.2.9.6. Complete additional training as directed by the AFECO.

1.2.10. **Host Installation Commander, Wing Commander (or equivalent).**

1.2.10.1. Appoints the Host APO, (T-1).

1.2.10.2. Appoint Tenant APOs in the Host Tenant Support Agreement (HTSA), as necessary.

1.2.11. **Host/Tenant Accountable Property Officer (APO).** Each Host/Tenant APO will:

1.2.11.1. Be appointed by the Host Installation Commander, Wing Commander (or equivalent), (T-1).

1.2.11.2. Serve as the accountable officer for all IT hardware and software on their installation, (T-1).

1.2.11.2.1. Appoint at least one primary and one alternate ECO, document acknowledgement of duties with handwritten or digital signatures, and provide a copy to the MECO, (T-1).

1.2.11.2.2. Ensure the designated APSR inventory provides accountability of all IT hardware assets, IAW **Chapter 2**, (T-1).

1.2.11.2.3. The Host APO is accountable for all IT assets on their installation, unless otherwise delegated in an HTSA, (T-1).

1.2.11.2.4. Ensure assets are accounted for throughout their lifecycle, (T-1).

1.2.11.2.5. Ensure an access controlled space is provided for the storage of non-issued assets (i.e. locking cabinet(s), locking room/closet, access-controlled segregated warehouse space, etc.), (T-1).

1.2.11.3. Designate primary and alternate Base Software License Managers (BSLM) (or equivalents) to manage the wing and/or base software license programs (to include applicable tenants) and inform their MAJCOM/A6 and Executive Agent for Enterprise Information Technology, (T-1).

1.2.11.3.1. Annually certify and document a software inventory was accomplished and the provisions of this AFMAN have been met. Provide a copy of the inventory to their MAJCOM/A6 and Executive Agent for Enterprise Information Technology, (T-1).

1.2.12. **Equipment Control Officer (ECO):**

1.2.12.1. Is appointed as primary or alternate by the Host/Tenant APO, (T-1).

1.2.12.1.1. Will be, at a minimum, the rank of E-5 or civilian equivalent, (T-3). There is not a rank/grade minimum for an alternate ECO.

1.2.12.1.2. Cannot be appointed Resource Advisor (RA) within the same unit in which they are performing duties as ECO, (T-1).

1.2.12.2. Will process the receipt, transfer and disposition of all Information Technology (IT) assets and complete necessary documentation to establish custodial responsibility, (T-1).

1.2.12.2.1. Assists Unit APOs in determining the ownership, reassignment or disposition of all Found-on-Base (FOB) IT assets.

1.2.12.2.2. Directs Unit APOs to conduct inventories in accordance with Attachment 3, *Information Technology (IT) Hardware Enterprise Inventory Plan*, (T-1).

1.2.12.2.3. Provides Unit APOs with asset labels.

1.2.12.2.4. Monitors AFECO collaboration sites for additional guidance and support.

1.2.12.3. Completes additional training as directed by the MECO.

1.2.12.4. Provides inventory assistance IAW Attachment 3, *Information Technology (IT) Hardware Enterprise Inventory Plan*.

1.2.13. **Base Software License Managers (BSLM).** Each BSLM will:

1.2.13.1. Ensure annual inventories are conducted for all non-enterprise software licenses for all organizations under BSLM purview, (T-0).

1.2.13.2. Collect an annual baseline of an inventory for all non-enterprise software licenses, (T-1).

1.2.13.3. Provide annual inventories to higher headquarters as required or requested.

1.2.14. **Unit APO.** Commanders (or their equivalent) are responsible for providing guidance and procedures to ensure adequate protection and oversight is afforded to IT assets under their control. Examples of a "commander equivalent" include a Director of Staff, a civilian director of an organization, or a commandant of a school organization. See AFI 38-101, *Air Force Organization*, for further guidance. Organization Commanders (or equivalent) will:

1.2.14.1. Serve as the Property Custodian IAW DoDI 5000.64, *Accountability and Management of DoD Equipment and Other Accountable Property,* section 3.2, paragraph f, (T-1).

1.2.14.2. Be responsible for the accountability of all IT hardware and software assets assigned to their unit, (T-1).

1.2.14.3. Ensure IT hardware and software assets are inventoried according to Attachment 3, *Information Technology (IT) Hardware Enterprise Inventory Plan*, (T-1).

1.2.14.4. Perform out-of-cycle inventories as directed, (T-1).

1.2.14.5. Monitor the acquisition, storage, utilization, and disposition of property within his or her assigned accountable area. Identify underutilized, impaired, or obsolete property and take appropriate actions to increase utilization or ensure disposition, (T-1).

1.2.14.6. Develop physical inventory plans and procedures, schedule physical inventories, and assist in their completion in accordance with DoDI 5000.64, *Accountability and Management of DoD Equipment and Other Accountable Property*, (T-1).

1.2.14.7. Manage all software licenses owned by the organization in support of the base software license management program, (T-1).

1.2.14.7.1. Annually certify and document to the BSLM a software inventory was accomplished, (T-1).

1.2.14.7.2. Ensure unused or underutilized software licenses are identified to the BSLM (or equivalents) for redistribution, reutilization, or disposition to comply with Executive Order 13589, *Promoting Efficient Spending*, (T-0).

1.2.14.7.3. Identify locally-owned software that does not have associated licenses, assemble proofs-of-purchase, and request replacement licenses from publishers, as needed. Develop plan of action to obtain compliance within 120 days, (T-1).

1.2.14.8. With the support of BSLM (or equivalents), ensure applicable training is conducted for users in support of unique software purchased or developed by organizations, (T-3).

1.2.14.9. Identify enterprise software license requirements and any management training requirements not covered in existing courses to the BSLM (or equivalents) for annual consolidation, (T-3).

Chapter 2

HARDWARE ASSET MANAGEMENT

2.1. Accountability of Information Technology (IT) Hardware Assets. Accountability and responsibility of IT hardware assets resides with the Commander, described in this manual as the Host/Tenant Accountable Property Officer (APO), and the Unit APO. Accountability takes place throughout the lifecycle of the asset.

2.1.1. **Accountability Determination.** In accordance with DoDI 5000.64, *Accountability and Management of DoD Equipment and Other Accountable Property*, Section 4, Air Force IT Property/Equipment will be accounted for using one of the three following processes based on the listed criteria applied to the asset/item.

2.1.1.1. **Accountable Property Record (APR) Process.**

2.1.1.1.1. An Information Technology (IT) asset/item will be accounted for using the APR process if any of the following criteria apply:

2.1.1.1.1.1. The asset/item has a unit acquisition cost of greater than or equal to $5,000, (T-0).

2.1.1.1.1.2. The asset/item was obtained via a capital lease, as defined in DoDFMR 7000.14-R, Volume 4, Chapter 6, *Property, Plant, and Equipment*, (T-0).

2.1.1.1.1.3. The asset/item is classified as defined in DoDI 5000.64, *Accountability and Management of DoD Equipment and Other Accountable Property*, (T-0).

2.1.1.1.1.4. The asset/item qualifies as a sensitive asset/item as defined in DoDI 5000.64, *Accountability and Management of DoD Equipment and Other Accountable Property*, (T-0).

2.1.1.1.1.5. The asset/item qualifies as pilferable as determined by SAF/CIO A6, (T-0).

2.1.1.1.1.6. The asset/item is categorized as Government Furnished Property (GFP) as defined in AFI 23-119, *Exchange, Sale, or Temporary Custody of Non-excess Personal Property,* (T-0).

2.1.1.1.2. Any IT asset/item meeting the criteria for this category will be managed using the designated Accountable Property System of Record (APSR), (T-0).

2.1.1.2. **Accountability Record (AR) Process.**

2.1.1.2.1. An Information Technology (IT) asset/item will be accounted for using the AR process if any of the following criteria apply:

2.1.1.2.1.1. The asset/item has a unit acquisition cost of less than $5,000 but is controlled or managed at the asset/item level IAW DoDI 4151.19, *Serialized Item Management (SIM) for Life-Cycle Management of Materiel*, (T-0).

2.1.1.2.1.2. The asset/item has the potential to store personally identifiable information (PII), (T-0).

2.1.1.2.1.3. The asset/item was obtained via an operating lease, as defined in DoDFMR 7000.14-R, Volume 4, Chapter 6, *Property, Plant, and Equipment*, (T-0).

2.1.1.2.1.4. Network and data management infrastructure whose unit cost is less than $5,000, (T-1).

2.1.1.2.2. Any IT asset/item meeting the criteria for this category can be managed using the designated APSR, or in a managerial system which has been designated by SAF/CIO A6, (T-0).

2.1.1.3. **Accounting for Information Technology (IT) Property/Equipment that does not meet the criteria for the APR or AR processes.**

2.1.1.3.1. For an IT asset/item that does not meet any of the criteria described in sections 2.1.1.1. or 2.1.1.2., the AF does not require accountability and tracking, and does not preclude an organization from doing so.

2.1.1.4. **Information Technology (IT) Components of a Weapon System or other Similar Capability.**

2.1.1.4.1. IT assets that are components of a Weapon System or other similar capability will be managed by this policy if both of the following apply:

2.1.1.4.1.1. The weapon system is not being managed in another APSR, per AFI 23-111, *Management of Government Property in Possession of the Air Force*, and AFI 21-103, *Equipment Inventory, Status and Utilization Reporting* (T-1), and

2.1.1.4.1.2. The IT components meet the requirements of paragraph 2.1.1.1. or paragraph 2.1.1.2. of this manual, (T-1).

2.2. Procurement of Information Technology (IT) Hardware Assets.

2.2.1. All AF IT hardware (including PWCS) will be procured using applicable AF Information Technology Commodity Council (ITCC) enterprise buying programs via AFWay at **https://www.afway.af.mil**, (e.g. Client Computing Solutions Quantum Enterprise Buy [CCS QEB], Digital Printing & Imaging [DPI], Cellular Services & Devices BPAs). All AF IT hardware not purchased through ITCC buying programs (CCS, DPI, & CSD BPAs), are mandated to use the NETCENTS-2 contracts, which enable delivery of products, services and solutions that adhere to the AF Enterprise Architecture, (T-1).

2.2.1.1. All requests for servers must comply with current National Defense Authorization Act as depicted in AFI 33-150. A DOD unique identifying number must accompany the acquisition.

2.2.1.2. The MAJCOM/A6s (or equivalents) may approve a QEB or DPI waiver via AFWay process, however MAJCOMs and Program Offices must use either AFWay-approved vendors or a NETCENTS-2 contract to meet their mission requirements, (T-1).

2.2.2. Ensure complete information is provided for shipping labels for ordered equipment. Obtain confirmation that procurement officials specify, as a contractual requirement, that "Ship To" and "Mark For" information is detailed on the shipping labels. This will alleviate problems with the receipt and acceptance processing of new hardware assets.

2.2.2.1. "Mark For" information will contain; Contract Number, Purchase Order Number, Address, Phone Number, E-mail Address, Resource Manager Name, and Unit APO (when applicable).

2.2.2.2. "Ship To" information will contain the complete delivery address. This includes the ECO name. This will correspond to the DoD Activity Address Code (DoDAAC) and the system of record for real property (ACES-RP).

2.2.2.3. Accountable IT hardware assets purchased through Government Purchase Card (GPC) must be added to the Accountable Property System of Record (APSR). ECOs must ensure the correct MAJCOM code is entered into the APSR for all asset(s) in their Primary Asset Account. The MAJCOM code must correctly identify the owning command, which may differ from the host base's command, (T-2).

2.2.2.4. End user devices shall be refreshed IAW recommended frequency outlined in Table 2.1.

Table 2.1. End User Device Refresh Rate.

Device Type	Recommended
Desktop	5 years
Laptop	4 years
Tablet	4 years
Cell Phone	2 years
Printer: Stand-alone	5 years
Printer: Multi-Functional Device	5 years

*Based on average warranties

2.3. Receipt and Acceptance of Information Technology (IT) Hardware Assets.

2.3.1. IT asset accountability must be established by formal receipt and acceptance in an accountable property system of record according to DoDI 5000.64, *Accountability and Management of DoD Equipment and Other Accountable Property*. AF IT asset accountability will be established in a timely manner by the following:

2.3.1.1. Receive and secure any assets until proper accountability via the Accountable Property System of Record (APSR) is established, (T-0).

2.3.1.1.1. The ECO or supporting personnel will enter newly received IT assets into the designated APSR. When received by anyone other than the ECO, the ECO will be notified of the asset(s) delivery. The asset will be secured and the asset(s) key supporting documentation (KSD) will be provided for inclusion to the APSR within 7 working days of receipt and acceptance. Capital assets must be recorded by the end of the month or within 7 calendar days, whichever is sooner, (T-0). Prior ECO approval is required when deviating from the standard ECO asset(s) delivery process.

2.3.1.2. Ensure unique asset identification is established for each item according to Serialized Item Management (SIM) and Item Unique Identification (IUID) guidance in AFI 63-101/20-101, *Integrated Life Cycle Management,* (T-0).

2.4. Sustainment of Information Technology (IT) Hardware Assets.

2.4.1. **Inventory.**

2.4.1.1. **Inventory Purpose.** The purpose of an inventory is to ensure that all assets in an asset account exist and can be readily located, as well as to ensure that any assets that are in the possession of the Air Force are being accounted for in accordance with applicable property and financial management policies.

2.4.2. **Inventory Frequency.**

2.4.2.1. Assets/items meeting the accountability criteria stated in section 2.1.1.1. will be inventoried annually, (T-0).

2.4.2.2. Assets/items meeting the accountability criteria stated in section 2.1.1.2. will be inventoried every three years, (T-0).

2.4.2.3. Assets/items meeting the accountability criteria in section 2.1.1.3. have no prescribed inventory frequency.

2.4.3. **Inventory Requirements.** Specific guidance on the minimum requirements applicable to all units in the Air Force for the inventory of IT Property/Equipment can be found in Attachment 3, *Information Technology (IT) Hardware Enterprise Inventory Plan*.

2.4.4. **Reports of Survey.**

2.4.4.1. Required if the lost, damaged, stolen or destroyed asset met the criteria for an accountable property record (APR), (T-0).

2.4.4.2. Required for any piece of property where it has been determined the loss, damage theft or destruction event constitutes a pattern of gross negligence, (T-0).

2.4.4.3. **Managing Capital Assets.** *The Chief Financial Officers (CFO) Act of 1990, 31 U.S.C. §§901-903*, specifies financial reporting and acquisition cost depreciation is required for equipment meeting the capitalization threshold as stated in DoDFMR 7000.14-R, Volume 4, Chapter 6, *Property, Plant, and Equipment*, (T-0).

2.4.4.3.1. Acquisition cost, which is what depreciation is based on, includes all costs incurred to bring the asset to a form and location suitable for its intended use (e.g., amounts paid to vendors, transportation to point of initial use, handling and storage costs, interest costs paid, and direct and indirect production costs).

2.4.4.4. **Contractor Guidance.**

2.4.4.4.1. Establish the extent of contractor liability in the provisions of the applicable contract’s government property clause according to AFI 23-111, *Management of Government Property in Possession of the Air Force*.

2.5. Disposition of Information Technology (IT) Hardware Assets.

2.5.1. **Transfer.**

2.5.1.1. When transferring equipment, all documentation applicable to the lifecycle of that asset (i.e. acquisition documentation, invoices, etc.) must be transferred along with that asset to the gaining organization, whether internal or external to the Air Force, (T-0).

2.5.2. **Disposal.**

2.5.2.1. A memorandum of agreement (MOA) between the Host installation and their regional DLADS facility will be formalized to document the processes and procedures for how that installation will interact with DLADS for the disposal of IT hardware assets.

2.5.2.2. Elements of this MOA may be incorporated into the HTSA.

2.5.2.3. Prior to disposal, the asset will have:

2.5.2.4. Met all IT hardware sanitization requirements, (T-0).

2.5.2.5. All applicable documentation related to the disposal process completed and signed, (T-0).

Chapter 3

SOFTWARE ASSET MANAGEMENT

3.1. Software Assets General Guidance and Procedures.

3.1.1. All software will be accounted for, (T-0). The intent of this chapter is to outline the requirements for software management, to include Internal Use Software (IUS).

3.1.2. All software will be accounted for by the acquiring or accountable organization, (T-0).

3.1.3. This chapter has been divided into 3 sections:

3.1.3.1. Management of Non-Enterprise Software, intended to provide requirements for what is expected from organizations purchasing software that is not already managed as a component of an Enterprise License Agreement or provided from the Air Force Standard Desktop Configuration (SDC).

3.1.3.2. Management of Enterprise Software, intended to provide the minimum set of requirements for how Enterprise-provided software should be managed and accounted for.

3.1.3.3. IUS Accountability, intended to provide the minimum set of requirements for what should be managed as IUS and the expectations associated with that management.

3.2. General Guidelines for Acquisition of Software.

3.2.1. All AF software will be procured using applicable buying programs (in order of precedence):

3.2.1.1. AF Enterprise License Agreements (ELA), (T-1).

3.2.1.2. DoD/Joint Enterprise License Agreements (JELA), (T-1).

3.2.1.3. DoD Enterprise Software Initiative (ESI) blanket purchase agreements, (T-1).

3.2.1.4. General Services Administration (GSA) schedules, (T-1).

3.2.1.5. Other vendor-authorized sources, (T-1).

3.2.2. To ensure that proper accountability can be performed on the purchased license(s), documentation verifying the acquisition cost of the license(s) must be retained by the acquiring or accountable organization, (T-0).

3.2.2.1. Documentation may include, but is not limited to; GPC receipts, Purchase Orders, Contract Agreements, etc.

3.2.2.2. Documentation verifying the acquisition cost of the software must be maintained in a readily available location during the applicable retention period, as described in DoD FMR 7000.14-R, Vol 1, Chapter 9, *Financial Records Retention*, to permit the validation of information pertaining to the asset, such as the purchase cost, purchase date, and cost of enhancements, (T-0).

3.3. Management of Non-Enterprise Commercial Software.

3.3.1. Receipt and Acceptance.

3.3.1.1. Proof of software purchase (i.e. purchase order, receipt, shipping order, etc.) will be kept on file with the BSLM as a component of the asset record, (T-0).

3.3.1.2. Proof of government ownership of software (End User License Agreement, contract clauses, etc.) will be kept on file with the BSLM as a component of the asset record, (T-0).

3.3.1.3. Proof of software purchase and proof of government rights to the software will be retained regardless of dollar value of the purchase, (T-0).

3.3.1.4. The asset record will be created in the designated management system or Accountable Property System of Record (APSR) within 7 working days of receipt and acceptance by the government or by the end of the calendar month, whichever is shorter, (T-0).

3.3.2. General Management of Use.

3.3.2.1. The BSLM will ensure licenses no longer needed by the intended user are removed from their system and retained for future use/deployment (i.e. transfer of the user to new program, no longer a validated need, etc.), (T-1).

3.3.3. Inventory of Non-Enterprise Software.

3.3.3.1. Organizations will inventory all licensed software annually and, if available utilize auto-discovery tools, to track and report implemented software and license information, (T-0).

3.3.3.2. The Unit APO will certify the annual inventory with a handwritten or digital signature indicating completion of the inventory and submit to the BSLM (or equivalents), (T-0).

3.3.4. Management of Legal Use.

3.3.4.1. Organizations will audit all systems to ensure no illegal or unauthorized copies of software are installed. Sampling procedures may be used if active inventorying/auto discovery systems are available, (T-0).

3.3.4.2. Automated tools should be used to the maximum extent possible for tracking software installed on the base network where applicable.

3.3.5. Managing Software Reuse.

3.3.5.1. Redistribution of excess or superseded software may occur if it:

3.3.5.1.1. Is permitted under the license agreement or upgrade policy for that software.

3.3.5.1.2. Is not classified.

3.3.5.1.3. Did not provide direct security protection to systems that processed classified information.

3.3.5.1.4. Is not directly related to or associated with a weapon system, intelligence system, command and control system, communications system, or tactical system.

3.3.5.1.5. Still operates as intended.

3.3.5.2. The asset record, and all documentation associated with it, must be transferred to the gaining organization along with the asset, (T-0).

3.3.6. **Managing Software Disposal.**

3.3.6.1. Dispose of excess or superseded software not redistributed by one of the following methods and according to license agreements:

3.3.6.1.1. Return the software package (distribution media, manuals, etc.) to the company that developed the software.

3.3.6.1.2. Destroy the software and license keys according to the provisions of the licensing agreement.

3.3.6.2. Document the method of destruction to establish an audit trail, (T-0).

3.4. Management of Enterprise Software.

3.4.1. At a minimum:

3.4.1.1. Legal use of enterprise licenses will be monitored by the Base Software License Manager (BSLM) to ensure usage does not exceed quantities purchased, (T-0).

3.4.1.2. The BSLM will perform and annual inventory of Enterprise software licenses reconcile them against contract information to maintain accountability of what the government has purchased as well as to ensure adherence to legal use per contract terms, (T-1).

3.5. Internal Use Software (IUS) Accountability.

3.5.1. **Description.**

3.5.1.1. IUS is:

3.5.1.1.1. Acquired or developed to meet internal or operational needs.

3.5.1.1.2. A stand-alone application, or the combined software components of an Information Technology (IT) system that can consist of multiple applications, modules, or other software components integrated and used to fulfill internal or operational need.

3.5.1.1.3. Used to operate the programs (e.g. financial and administrative software).

3.5.1.1.4. Used to produce goods and provide services (e.g. maintenance work order management).

3.5.1.1.5. Developed to or obtained for internal use and subsequently provided to other federal entities with or without reimbursement.

3.5.1.2. IUS is not:

3.5.1.2.1. Software that is integrated into and necessary to operate equipment rather than perform an application (i.e., an operating system).

3.5.2. **General Accountability.** Accountability of Internal Use Software (IUS) will be:

3.5.2.1. Established and maintained:

3.5.2.1.1. At the end of the development phase for government- or contractor-developed IUS, (T-0).

3.5.2.1.2. Upon government acceptance of commercial off-the-shelf (COTS) IUS, (T-0).

3.5.2.1.3. Upon the completed transfer to another unit/organization within the Air Force, (T-0).

3.5.2.1.4. By the acquiring organization in accordance with DoDFMR 7000.14-R, Volume 4, Chapter 6, *Property, Plant, and Equipment,* (T-0).

3.5.2.2. Established for capitalized IUS in the designated APSR, (T-0).

3.5.2.3. Established for IUS which does not meet the criteria for capitalization in the designated APSR or designated managerial system, (T-0).

3.5.2.4. Established for IUS in development in accordance with section 3.5.4., (T-0).

3.5.2.5. Enabled through unique identification (UID) standards, in accordance with DoDI 8320.03, *Unique Identification (UID) Standards for Supporting the DoD Information Enterprise,* (T-0).

3.5.2.6. Maintained by the accountable organization until formal relief of accountability through authorized means, such as transfer or disposal, (T-0).

3.5.3. **Accountable Records.**

3.5.3.1. The accountable organization will establish accountable records in the designated Accountable Property System of Record (APSR) for all capitalized Internal Use Software (IUS), (T-0).

3.5.3.1.1. A single record will be established for each IUS purchase or acquisition and all costs incorporated in accordance with the DoDFMR 7000.14-R, Volume 4, Chapter 6, *Property, Plant, and Equipment*, guidance, (T-0).

3.5.3.1.2. A single record will be established for each stand-alone COTS license with a unit cost that exceeds the capitalization threshold and is not a component of a developed system, (T-0).

3.5.3.1.3. A single record will be established for each distinct manufacturer part number on each purchase order for a bulk license purchase for COTS software, (T-0).

3.5.3.2. The accountable organization will maintain accountable records for non-capital IUS in the designated APSR or designated managerial system, (T-0).

3.5.3.3. The accountable organization will maintain accountable records for the life of the asset and will retain the records:

3.5.3.3.1. For 7 years after the end of the operational life of the developed IUS, (T-1).

3.5.3.3.2. For 7 years following the end of legal use for capitalized COTS, (T-1).

3.5.4. **Accountability of Software-in-Development.**

3.5.4.1. No formal property accountability (i.e., accountable property record) is established until Internal Use Software (IUS) development is completed, in accordance with section 3.5.2., (T-0).

3.5.4.2. Accountability is established in the APSR at the end of the development phase after the IUS developed has been final tested to verify that it meets specifications, (T-0).

3.5.4.2.1. The end of the development phase for major automated information systems will be the Full Deployment Decision (FDD), as described in DoDI 5000.02, *Operation of the Defense Acquisition System*, (T-0).

3.5.4.2.2. The end of the development phase for IUS that is not designated as major automated information systems will be the date that initial operating capability is established, (T-0).

3.5.4.2.3. IUS accountability also applies to National Security Systems, in accordance with DoDD 8000.01, *Management of the Department of Defense Information Enterprise (DoD IE)*, (T-0).

3.5.4.3. APSR records must be updated to reflect the physical changes made to the IUS and the associated costs when IUS enhancements, improvements, or other modifications occur, (T-0).

3.5.5. **Accountability of Commercial Internal Use Software (IUS) Licenses.**

3.5.5.1. Property accountability is required for commercial off-the-shelf (COTS) software licenses that meet all of the following criteria:

3.5.5.1.1. The COTS licenses are purchased for deployment to end user personal computing devices or computer servers, (T-0).

3.5.5.1.2. The COTS is purchased through a financial transaction or received as an IUS asset transfer from another entity, (T-0).

3.5.5.2. The IUS asset for a COTS license is the license agreement and record of ownership, such as the purchase order, contract, or assignment of licenses documentation for a transfer, (T-0).

3.5.5.3. The accountable organization will establish accountability for COTS IUS licenses:

3.5.5.3.1. Upon acceptance of the software order by the receiving organization for software licenses procured directly by the government, (T-0).

3.5.5.3.2. Upon the date the transfer occurs for commercial off-the-shelf (COTS) licenses received by the Air Force as an asset transfer from another entity, (T-0).

3.5.5.4. For bulk purchased software, units will record and track bulk license purchases as follows:, (T-0).

3.5.5.4.1. If the cost is below the capitalization threshold, the bulk license purchase should be expensed, (T-0).

3.5.5.4.2. For any purchase order or license transfer for which the total value of the COTS software licenses exceeds the capitalization threshold, the bulk license purchase should be capitalized, (T-0).

3.5.5.4.3. For COTS licenses procured through a bulk purchase and intended for use in or integration into developed Internal Use Software (IUS), the software licenses are accountable as part of the bulk license purchase and should not be allocated or otherwise associated with any developed IUS, (T-0).

3.5.5.5. COTS software licenses purchased for use in or integration with developed IUS will be included with the developed IUS, unless the licenses are procured through a bulk license purchase, in which case the provisions for bulk license purchases apply. Individual license accountability is not applicable, (T-0).

3.5.5.5.1. For bulk COTS software costs that will be capitalized, capitalized costs should include the amount paid to the vendor for the software and material internal costs incurred to implement the COTS software and otherwise make it ready for use. License maintenance, conversion costs, or upgrade purchases should be treated according to the DoDFMR 7000.14-R, Volume 4, Chapter 6, *Property, Plant, and Equipment*, and are typically expensed, (T-0).

3.5.5.6. Accountability for commercial off-the-shelf (COTS) licenses ceases when:

3.5.5.6.1. The final term expires and the license owner has complied with the publisher terms and conditions for terminating the license for term license agreements, (T-0).

3.5.5.6.2. A perpetual license is removed from inventory (e.g., uninstalled from computer(s) or upon the appropriate disposal of the hard drive(s) to which the software was installed) and when the disposal of the license is made in accordance with the license terms and the conditions for terminating, transferring, or otherwise retiring the license are completed, (T-0).

3.5.5.6.3. The accountable organization will ensure that documentary evidence is recorded and maintained in accordance with Air Force records management requirements, (T-0).

3.5.6. **Accountability of Internal Use Software (IUS) Delivered As A Service.**

3.5.6.1. Any license provided to Air Force users as a service (i.e. cloud computing, software as a service, or other “as a service” software subscriptions) will only be considered accountable IUS assets if an Air Force organization is designated as the licensee and the license owner retains the right to take control of the license independent of the hosting arrangement, (T-0).

3.5.6.2. Any license that is provided to AF users on an AF computer or on a computer owned by a third party and is not licensed to the AF will not be accountable as a DoD IUS asset, (T-0).

3.5.6.3. COTS IUS that is provided to the AF as a service that meets the requirement for accountability as an IUS asset, in accordance with section 3.5.1., will be accountable using the provisions for accountability for COTS licenses in section 3.5.5., (T-0).

3.5.7. **Internal Use Software (IUS) Inventory.**

3.5.7.1. All accountable organizations must maintain up-to-date inventory records of IUS for which they are accountable, (T-0).

3.5.7.2. In order to support maintenance of an up-to-date inventory of IUS and meet financial reporting requirements, accountable organizations must process all inventory changes (i.e., receipts of IUS, transfers between DoD Components, or disposition) within 7 calendar days or the end of the month in which the financial event occurs, whichever is sooner, (T-0).

3.5.7.3. The accountable organization must take an inventory of accountable Internal Use Software (IUS) no less than annually by fiscal year end to assess the accuracy of IUS asset records, update IUS asset records, assess any IUS property loss experienced, and provide the status of verified assets for fiduciary reporting purposes, (T-0).

3.5.7.4. A minimum 98 percent inventory accuracy rate will be achieved and maintained for capitalized IUS asset records, (T-0).

3.5.7.5. Any property loss discovered during the inventory should be reported and an inventory adjustment should be performed in accordance with record adjustment procedures, (T-0).

3.5.7.6. An annual “true-up” of licenses is sufficient for inventory validation of affected IUS licenses. The true-up may be utilized in place of the 98 percent accuracy rate with only those impacted, non-capital IUS assets, (T-0).

3.5.7.7. Accountable organizations will retain details of the result of their most current annual inventory, (T-0).

3.5.8. **Disposal.**

3.5.8.1. To properly transfer, dispose of, donate, or reuse commercial Internal Use Software (IUS), accountable organizations must adhere to product licensing agreements to avoid potential fines or litigation, (T-0).

3.5.8.1.1. Before the accountable organization disposes of commercial IUS, legal counsel should review all IUS licenses for any limitations or potential liability, (T-0).

3.5.8.1.2. Accountable organizations must consult all relevant parties before any IUS disposition activity, (T-0).

3.5.8.2. The IUS disposal process involves turn-in to the Defense Logistics Agency Disposition Services and, in some cases, destruction, (T-0).

3.5.8.2.1. The disposal process should be executed in accordance with DoD Manual 4160.21, *Defense Materiel Disposition*, unless there is a conflict with the terms and conditions of the software license agreements or contracts, in which case the software license agreement and contract will take precedence, (T-0).

3.5.8.3. When Internal Use Software (IUS) is transferred, reassigned, exchanged, or sold to government or non-government organizations, the original documentation and media disks for the IUS must accompany it if the IUS was acquired commercially, (T-0).

3.5.8.3.1. In these instances, the original owner of the IUS must execute proper license transfer documentation with the manufacturer, (T-0).

3.5.8.4. Disposal is not complete unless all copies of the targeted IUS are uninstalled from the accountable organization's network through uninstall procedures or proper disposition of the computer hardware or hard drive upon which the software is installed, (T-0).

3.5.8.5. The accountable organization will document the destruction, or vendor return, of IUS and report it to an adjunct APO. This will include a statement verifying that all media, licenses, and documentation have been destroyed or returned to the vendor, (T-0).

3.5.9. **Valuation.**

3.5.9.1. Valuation is required for Capital Internal Use Software (IUS), (T-0).

3.5.9.1.1. All IUS will be capitalized when meeting the following criteria:

3.5.9.1.1.1. Total acquisition cost is greater than or equal to $250,000, (T-0).

3.5.9.1.2. Useful life of the IUS is greater than or equal to 2 years, (T-0).

3.5.9.2. IUS will be capitalized at full cost, which is comprised of the acquisition cost and other associated costs as outlined in Table 3.1., (T-0).

Table 3.1. Internal Use Software (IUS) Capitalization Cost Determination.

Project Phase	Task	Treatment
Preliminary Design: Conceptual Planning/Planning & Requirements	Project Evaluation or Need Determination	Expense
	Concept Formulation and Testing	Expense
	Evaluation and Testing of Alternatives	Expense
	Project Approval	Expense
Software Development: Design/Development & Testing/Implementation	Design, Including Software Configuration and Software Interfaces	Capitalize
	Coding	Capitalize
	Installation to Hardware	Capitalize
	Project Personnel Costs	Capitalize
	Testing, Including Parallel Processing	Capitalize
	Quality Assurance Testing	Capitalize
	Technical Documentation, Including User Manuals	Capitalize
	Data Conversion Software	Expense
	General and Admin Costs	Expense

Operational Software: Operations & Maintenance / Disposition	Enhancements	Capitalization Criteria Dependent
	Training	Expense
	Data Conversion, Includes Cleansing, Deleting, and Repackaging of Data	Expense
	Help desk	Expense
	Application Maintenance/Bug Fix	Expense

3.5.9.3. When acquisition cost is unknown, reasonable estimates of the historical acquisition cost may be used, (T-0).

3.5.10. Additional Resources. For additional detail on IUS Accountability, refer to DoDI 5000.76, *Accountability and Management of Internal Use Software (IUS)*.

BRADFORD J. SHWEDO, Lt Gen, USAF
Chief, Information Dominance and
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Executive Order 13103, *Computer Software Piracy*, 30 September 1998

Executive Order 13589, *Promoting Efficient Spending*, 9 November 2011

The Copyright Act of 1976

The Chief Financial Officers (CFO) Act of 1990, 31 U.S.C. §§901-903

FAR, Subpart 7.5, *Inherently Governmental Functions*, FAC 2005-97, 13 January 2017

DFARS, Subpart 217.70, *Exchange of Personal Property*, 28 December 2017

DoDFMR, 7000.14-R, Vol 1, Chapter 9, *Financial Records Retention*, February 2016

DoDFMR 7000.14-R, Volume 3, Chapter 8, *Standards for Recording and Reviewing Commitments and Obligations*, February 2016

DoDFMR 7000.14-R, Volume 4, Chapter 6, *Property, Plant, and Equipment*, June 2009

DoDD 8000.01, *Management of the Department of Defense Information Enterprise (DoD IE)*, 17 March 2016

DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG*), 14 April 2004

DoDI 4151.19, *Serialized Item Management (SIM) for Life-Cycle Management of Materiel*, 9 January 2014

DoDI 5000.02, *Operation of the Defense Acquisition System*, 7 January 2015

DoDI 5000.64, *Accountability and Management of DoD Equipment and Other Accountable Property*, 27 April 2017

DoDI 5000.76, *Accountability and Management of Internal Use Software (IUS)*, 2 March 2017

DoDI 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)*, 21 April 2016

DoDI 8320.02, *Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense*, 5 August 2013

DoDI 8320.03, *Unique Identification (UID) Standards for Supporting the DoD Information Enterprise*, 4 November 2015

DoDI 8330.01, *Interoperability of Information Technology (IT) Including National Security Systems (NSS)*, 21 May 2014

DoDI 8500.01, *Cybersecurity*, 14 March 2014

DoD Manual 4160.21, *Defense Materiel Disposition*, 22 October 2015

DoDM 5400.-7-R_AFMAN33-302, *Freedom of Information Act Program*, 21 October 2010

ISO/IEC 19770, *Software Asset Management (SAM)*

ISO/IEC 20000, *Information Technology - Service Management*

AFPD 10-6, *Capabilities Requirements Development*, 6 November 2013

AFPD 17-1, *Information Dominance Governance and Management*, 12 April 2016

AFPD 17-2, *Cyberspace Operations*, 12 April 2016

AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program,* 2 June 2015

AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT),* 2 February 2017

AFI 17-110, *Air Force Information Technology Portfolio Management and IT Investment Review*, 23 December 2008

AFI 17-130, *Cybersecurity Program Management,* 31 August 2015

AFI 17-210, *Radio Management,* 26 May 2016

AFI 21-103, *Equipment Inventory, Status and Utilization Reporting,* 16 December 2016

AFI 23-111, *Management of Government Property in Possession of the Air Force,* 29 October 2013

AFI 23-119, *Exchange, Sale, or Temporary Custody of Non-excess Personal Property*, 5 June 2001

AFI 38-101, *Air Force Organization*, 31 January 2017

AFI 63-101/20-101, *Integrated Life Cycle Management*, 9 May 2017

AFI 65-201, *Managers' Internal Control Program Procedures*, 9 February 2016

AFI 90-201, *The Air Force Inspection System*, 21 April 2015

AFMAN 17-1301, *Computer Security (COMPUSEC),* 10 February 2017

AFMAN 17-1402, *Air Force Clinger-Cohen Act (CCA) Compliance Guide*, 24 October 2012

AFMAN 23-220, *Reports of Survey for Air Force Property*, 1 July 1996

AFMAN 33-363, *Management of Records,* 1 March 2008

Prescribed Forms

No forms are prescribed by this publication

Adopted Forms

DD Form 200, *Financial Liability Investigation of Property Loss*

DD Form 250, *Material Inspection and Receiving Report*

DD Form 1149, *Requisition and Invoice/Shipping Document*

DD Form 1348-1A, *Issue Release/Receipt Document*

AF Form 847, *Recommendation for Change of Publication*

AF Form 2519, *All Purpose Checklist*

Abbreviations and Acronyms

AF—Air Force

AFECO—Air Force Equipment Control Officer

AFEMS—Air Force Equipment Management System

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFMC—Air Force Materiel Command

AFPD—Air Force Policy Directive

AFPSC—Air Force Space Command

AFWay—Air Force Way

AIM—Asset Inventory Management

APSR—Accountable Property System of Record

BSLM—Base Software License Manager

C4—Command, Control, Communications, and Computers

CAGE—Commercial and Government Entity code

CIO—Chief Information Officer

COTS—Commercial Off-the-Shelf

CS—Communications Squadron

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDFMR—Department of Defense Financial Management Regulation

DoDI—Department of Defense Instruction

DRU—Direct Reporting Unit

ECO—Equipment Control Officer

ELA—Enterprise License Agreement

E.O—Executive Order

ESI—Enterprise Software Initiative

FAR—Federal Acquisition Regulation

FOA—Field Operating Agency

IT—Information Technology

ITAM—Information Technology (IT) Asset Management

IUS—Internal Use Software

MAJCOM—Major Command

MECO—Major Command Equipment Control Officer

MOA—Memorandum of Agreement

OPR—Office of Primary Responsibility

PWCS—Personal Wireless Communications Systems

SAF—Secretary of the Air Force

SPI—Software Process Improvement

Terms

Acceptance — A formal certification that the goods or services have been received and that they conform to the terms of the contract. See Federal Acquisition Regulation Part 46 for contractual requirements and procedures that constitute acceptance.

Accountability — The obligation imposed by law, lawful order, or regulation, accepted by an organization or person for keeping accurate records and to ensure control of property, documents or funds, with or without physical possession. The obligation, in this context, refers to the fiduciary duties, responsibilities, and obligations necessary for protecting the public interest; however, it does not necessarily impose personal liability upon an organization or person.

Accountable Officer — An individual appointed by proper authority who maintains items and/or financial records in connection with government property, irrespective of whether the property is in his or her possession for use or storage, or is in the possession of others to whom it has been officially entrusted for use or care and safekeeping. In all cases, the accountable officer is responsible for establishing and maintaining financial property control records, controlling the processing of supporting documentation, and maintaining supporting document files. The primary accountable officers under the Air Force ROS System include: chief of supply, medical supply officer, munitions officer, fuels officer, communications and information systems officer, civil engineer, etc.

Accountable Property Officer (APO) — An individual who, based on his or her training, knowledge, and experience in property management, accountability, and control procedures, is appointed in writing through the DoD Component procedures to establish and maintain an organization’s accountable property records, systems, or financial records, in connection with government property, irrespective of whether the property is in the individual's possession.

Accountable Property Record — The record contained within the APSR.

Accountable Property System of Record (APSR) — The government system used to control and manage accountable property records. A subset of existing organizational processes related to the lifecycle management of property; the system that is integrated with the core financial system. The APSR may also control and manage accountability records as described in Paragraph 2.1.

Accountability Record — A record maintained for managerial rather than financial reporting purposes. Accountability records should be used when the property does not meet the accountable property record requirements (Paragraph 2.1) but does require active management based on other than financial criteria.

Acquisition — Acquiring hardware, supplies, or services: Through purchase, lease, or other means, including transfer or fabrication, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated; or by contract with appropriated funds of supplies or services.

Acquisition Cost — The amount, net of both trade and cash discounts, paid for the property, plus transportation costs and other ancillary costs. See "full cost."

Automated Inventory Tool (AIT) — The family of technologies that improves the accuracy, efficiency, and timeliness of material identification and data collection. AIT media and devices include, but are not limited to, linear and two-dimensional bar code symbols and their readers; magnetic stripe cards; integrated cards, (i.e., smart cards; optical memory cards); radio frequency identification (active and passive); contact memory-button devices; and magnetic storage media.

Capital Asset — An asset that meets or exceeds the capitalization threshold found in DoDFMR 7000.14-R, Volume 4, Chapter 6, *Property, Plant, and Equipment,* for the DoD Component**.**

Capital Lease — Leases that transfer substantially all the benefits and risks of ownership to the lessee. If at its inception, a lease meets one or more of the following criteria, the lease is considered a capital lease: 1) the lease transfers ownership of the property to the lessee by the end of the lease term, 2) the lease contains an option to purchase the leased property at a bargain price, 3) the lease term (non-cancelable portion, plus all periods, if any, representing renewals or extensions that can reasonably be expected to be taken) is equal to or greater than 75 percent of the estimated economic life of the leased property, and 4) the present value of rental and other minimum lease payments, excluding that portion of the payments representing executory cost, equals or exceeds 90 percent of the fair value of the leased property. See DoDFMR 7000.14-R, Volume 4, Chapter 6, *Property, Plant, and Equipment,* for procedures and additional information.

Command, Control, Communications, and Computer (C4) Systems — Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control, across the range of military operations. Also called "communications and information systems."

Commercial Off—the-Shelf (COTS) Software - Software developed, tested, and sold by commercial companies to the general public. This software meets operational requirements without modification or alteration to perform on a DOD network or computer. Examples include word processors, databases, application generation, drawing, compiler, graphics, communications, and training software.

Computer System — A functional unit, consisting of one or more computers and associated software, that (1) uses common storage for all or part of a program and also for all or part of the data necessary for the execution of the program; (2) executes user-written or user-designated programs; and (3) performs user-designated data manipulation, including arithmetic and logic operations. Note: A computer system is a stand-alone system or may consist of several interconnected systems. Personal computers, microcomputers, minicomputers, multi-user systems, all standard multi-user small computer requirements contract systems, text processors, word processors, intelligent typewriters, and workstations are examples of computer systems.

Contract — Any enforceable agreement, including rental and lease agreements and purchase orders, between an agency and a business concern for the acquisition of property or services.

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

End User Devices— Desktops, notebooks, tablets, accessories, mobile devices (e.g., blackberry, smart phones, pagers), phones (e.g., desk phones), that are used by end users.

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

Equipment — Personal property that is functionally complete for its intended purpose, durable, and nonexpendable. Equipment generally has an expected service life of two years or more; is not intended for sale; does not ordinarily lose its identity or become a component part of another article when put into use; has been acquired or constructed with the intention of being used.

Equipment Control Officer (ECO) — An individual appointed by the applicable Host/Tenant APO to manage and control Information Technology (IT) assets for an installation.

Found—on-Base (FOB) - Any IT hardware equipment found in the Unit APO-owned area that is not on the current inventory listing.

Full cost — A baseline value that includes all material costs incurred to acquire and bring the property to a form and location suitable for its intended use and, as applicable, depreciated over its useful life.

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.

Host APO — Accountable property officer appointed by the Installation Commander to manage the Information Technology Asset Management (ITAM) program for the Installation.

Information Technology (IT) — Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the DoD component. For the purposes of the preceding sentence, equipment is used by a DoD component if the equipment is used directly or is used by a contractor under a contract with the DoD component that (1) requires the use of such equipment; or (2), requires the use to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term Information Technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services) and related resources. Notwithstanding the above, the term information technology does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract (DoDD 8000.01, *Management of the Department of Defense Information Enterprise (DoD IE*).

Key Supporting Documents — Documentation needed by transaction type to support the relevant financial statement assertion. Examples include purchase invoices, contracts, DD Forms 1149, 1348-1A, 200, etc.

License Agreements — Contracts between the software publisher and the user that instructs and limits the software use. When purchasing software, the buyer only acquires a license to use it. The publisher retains the full rights to the software and has the sole right to its further distribution and reproduction.

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 over the life of the automated information system.

Maintenance — (1) All action taken to retain materiel in or to restore it to a specified condition. It includes: inspection, testing, servicing, classification as to serviceability, repair, rebuilding, and reclamation. (2) All supply and repair action taken to keep a force in condition to carry out its mission. (3) The routine recurring work required to keep a facility (plant, building, structure, ground facility, utility system, or other real property) in such condition that it is continuously utilized, at its original or designed capacity and efficiency, for its intended purpose. (4) The function of keeping C4 items of equipment in, or restoring them to, serviceable condition. Maintenance is not intended to increase the value, capabilities, or expected life of a system. Equipment maintenance includes servicing, repair, modification, modernization, overhaul, inspection, condition determination, corrosion control, and initial provisioning of support items. Maintenance includes both preventive and corrective actions. Software maintenance includes anticipating, detecting, and eliminating errors.

Major Command Equipment Control Officer (MECO) — The individual appointed by the MAJCOM, FOA, and DRU, or equivalent that oversees the management and control of IT assets within their area of responsibility.

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.

Personally Identifiable Information — Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother’s maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Physical Inventory— The verification of property existence, accountable property record completion, location, and quantity. The process may also involve verifying additional information, performing reconciliations, and modifying the accountable property records. Also see ASTM International E-2135-10ae1 for voluntary consensus standards on conducting a physical inventory.

Pilferable Items — Property that has a ready resale value or application to personal possession, and that are therefore especially subject to theft.

Property — Equipment, weapon systems, and other accountable property (e.g., administrative property, special tools, special test equipment). Other types of personal property, such as supplies, material, and records, are not included in this definition unless expressly stated as being included.

Receipt — A transmission or other acknowledgment made by a receiving entity to indicate that a message, good, or service has been satisfactorily received. Receipt is often denoted by signing a situation specific form, such as DD Forms 250, 1149, "Requisition and Invoice/Shipping Document," or 1348-1A, "Issue Release/Receipt Document."

Reconciliation — The process of aligning the physical count with the quantity posted to the accountable property records, researching discrepancies, and determining inventory accuracy, i.e., calculation of loss or overage rates.

Requirement — A need for a new or improved information processing capability that, when satisfied, increases the probability of operational mission success or decreases the cost of mission support.

Reuse— The process of developing or supporting a software-intensive system using existing software assets.

Software — (1) A set of Information Technology (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.

System— A set of IT components and their external peripherals and software interconnected with another set. Typical systems include notebook computers, desktop PCs, networked and distributed systems (e.g., servers, workstations, data management processors, etc.), mainframe and midsize computers and associated peripherals.

Tenant APO —Accountable property officer of a tenant organization for which the installation does not support Information Technology Asset Management (ITAM) for the tenant organization as stipulated in the Host Tenant Support Agreement.

Unit APO — The commander of an organization which has custodial responsibility for information technology assets.

Attachment 2

DESIGNATED ACCOUNTABLE PROPERTY SYSTEM OF RECORD (APSR) GUIDANCE

A2.1. Purpose and Scope. This attachment provides guidance for use of the designated APSR. SAF/CIO A6 has designated AFEMS-AIM as the Accountable Property System of Record for Information Technology (IT) hardware assets. The Air Force Medical Operations Agency (AFMOA) has designated the Defense Medical Logistics Standard Support (DMLSS) system as the medical War Reserve Material (WRM) IT hardware asset accountability system.

A2.2. AFEMS-AIM Roles and Responsibilities.

A2.2.1. **Primary and Alternate Major Command Equipment Control Officer (MECO).**

A2.2.1.1. Provides guidance and procedural policy to the ECOs regarding management of IT/Personal Wireless Communications Systems (PWCS) assets.

A2.2.1.2. Approves or rejects transfer of IT/PWCS assets between losing and gaining commands, (T-1).

A2.2.1.3. Reviews finalized excess reports completed by applicable ECOs and ensures appropriate action is accomplished.

A2.2.1.4. Coordinates on the establishment of a new Primary Asset Account and the IT/PWCS data system connectivity, as required.

A2.2.1.5. Manages the IT/PWCS Primary ECO user roles.

A2.2.1.6. Establishes accountability for IT/PWCS assets acquired through joint services PMs, as required.

A2.3.1. **Primary and Alternate Equipment Control Officer (ECO).**

A2.3.1.1. Loads all Information Technology (IT) and Personal Wireless Communications Systems (PWCS) asset records, (T-1).

A2.3.1.2. Ensures correct MAJCOM code is entered into AFEMS-AIM for all IT/PWCS assets in their respective DRA. Ensures the IT/PWCS asset status code(s) in AFEMS-AIM is updated as required.

A2.3.1.3. Reviews the IT asset status codes periodically to ensure the codes reflect the current status.

A2.3.1.4. Creates all new accounts within their DRA and modifies the applicable Primary and Alternate Equipment Custodians (EC), (T-1).

A2.3.1.5. Processes receipt, transfer, and disposition of Information Technology (IT) assets in AFEMS-AIM, (T-1).

A2.3.1.6. Assists the EC in determining the ownership of all Found on Base (FOB) assets, (T-2).

A2.3.1.7. Directs Unit APOs to conduct complete inventories of all assets assigned to the Unit APO (ECOs have the authority to lock Unit APO accounts until the inventories are completed), (T-1).

A2.3.1.8. Ensures all assets are labeled with CAGE Code, Part Number, and Serial Number, (T-1).

A2.3.1.8.1. If manufacturer labels do not contain proper identification, produces AFEMS-AIM-generated standard product (bar code) labels for the Unit APO, (T-1).

A2.3.1.8.2. If AFEMS-AIM-generated standard product labels cannot be produced, establishes local labels that contain proper identification and provide them to the Unit APO, (T-1).

A2.3.1.9. Adjusts inventories once loss/gain discrepancies have been reconciled, (T-2).

A2.3.1.10. Codes deployable IT/PWCS assets in the AFEMS-AIM database, (T-1).

A2.3.1.11. Prepares the necessary shipping documents for items that are excess and required by other services, (T-3).

A2.4.1. **Auditor - Requires AFECO approval.**

A2.4.1.1. Provides the capability to view AFEMS-AIM data and to produce Discoverer reports.

A2.5.1. **AFEMS-AIM User Guide.** For specific instructions on how to perform AFEMS-AIM functions, utilize the AFEMS-AIM User Guide link located on the AFECO Collaboration Site.

Attachment 3

INFORMATION TECHNOLOGY (IT) HARDWARE ENTERPRISE INVENTORY PLAN

A3.1. Purpose and Scope. The intent of this plan is to articulate the minimum requirements for performing asset/item inventories for IT hardware assets. Additional requirements that may be levied onto units by their parent MAJCOM/DRU/FOA organization will be articulated in a MAJCOM/DRU/FOA-specific Inventory Plan.

A3.2. Inventory Frequency.

A3.2.1. Assets meeting the criteria stated in paragraph 2.1.1.1. will be inventoried annually.

A3.2.2. Assets meeting the criteria stated in paragraph 2.1.1.2. will be inventoried every three years.

A3.3. Preparing for Inventory.

A3.3.1. To prepare for an asset inventory, a baseline of the asset account will be produced by the ECO and provided to the Unit APO.

A3.3.2. To assist in this process, the account owner can use a combination of asset discovery/automated inventory tools and manual identification of assets.

A3.3.2.1. The account owner can utilize enterprise asset discovery tools to perform a network scan to "discover" assets on the network that are within their account.

A3.3.3. This discovery cannot be done any earlier than one month prior to the inventory due date.

A3.3.4. One month of scanning will produce a list of assets that have been on the network at various times over that scanning period and this list can be included as a component of the inventory of a complete account.

A3.4. Performing the Inventory. To perform an asset inventory, the Unit APO:

A3.4.1. Will ensure that all assets in their account(s) have been identified.

A3.4.2. Will ensure that gains/losses against the inventory baseline are documented and reconciled.

A3.4.3. If using Automated Inventory Tool (AIT), the physical inventory can be performed only on those assets not identified using the AIT.

A3.5. Completing the Inventory. To complete an asset inventory, the Unit APO:

A3.5.1. Will ensure that the individual performing the inventory has signed, indicating that the inventory is complete and accurate.

A3.5.2. Will endorse the signed inventory with signature, accepting responsibility for the results.

A3.5.3. Will provide the completed, signed, and endorsed inventory in an electronic format to the installation ECO for record.

A3.6. Finalizing the Inventory. To finalize an asset inventory, the ECO will reconcile all gain/loss annotations in the designated Accountable Property System of Record (APSR).

A3.7. Random Sampling. Random sampling of the Information Technology (IT) asset enterprise will be performed by the AFECO to ensure that inventory requirements are being adhered to.