BY ORDER OF THE SECRETARY OF THE AIR FORCE

DEPARTMENT OF THE AIR FORCE MANUAL 17-1203

13 SEPTEMBER 2022

KIRTLAND AIR FORCE BASE Supplement

31 JANUARY 2023

Cyberspace

INFORMATION TECHNOLOGY ASSET MANAGEMENT (ITAM) AND ACCOUNTABILITY

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/CNS

Certified by: SAF/CNS (Venice Goodwine, SES)

Supersedes: AFMAN 17-1203, 18 May 2018

Pages: 88

(KIRTLANDAFB)

OPR: 377MSG/SCOL

Certified by: 377MSG/SC (Robert B. Rudolph, GS-14)

Supersedes: AFMAN17-1203_KIRTLANDAFBSUP, 2 November 2018

Pages: 88

This Department of the Air Force Manual (DAFMAN) implements Department of the Air Force Policy Directive (DAFPD) 17-1, *Information Dominance Governance and Management*, and supports DAFPD 17-2, Cyber Warfare Operations and AFPD 10-6, Capability Requirements Development. This DAFMAN provides the overarching guidance and direction for managing Department of the Air Force (DAF) Information Technology (IT) hardware and software assets as defined in overarching requirements outlined in DODI 5000.64, *Accountability and Management of DOD Equipment and Other Accountable Property*, DODI 5000.76, *Accountability and Management of Internal Use Software*, DOD FMR, 7000.14-R, Volume 4, Chapter 25, *General Equipment*, and DOD FMR, 7000.14-R, Volume 4, Chapter 27, *Internal Use Software*.

This DAFMAN is applicable to all civilian employees and uniformed members of the Regular Air Force, United States Space Force (USSF), the Air National Guard, and the Air Force Reserve. 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. Refer recommended changes and questions about this publication to the office of primary responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate chain of command. This publication may be supplemented at any level, but all supplements must be routed to the OPR of this publication for coordination prior to certification and approval. 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) 90-160, *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. 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 DAF. Compliance with Attachments **2, 3, 4 and 5** in this publication is mandatory. This publication requires the collection and/or maintenance of information protected by the *Privacy Act of 1974* authorized by Title 10 U.S.C., Sec 9013, Secretary of the Air Force.

(KIRTLANDAFB) This publication supplements Department of the Air Force Manual (DAFMAN) 17-1203, *Information Technology Asset Management (ITAM) and Accountability*. This supplement defines the responsibilities, and requirements for Kirtland Air Force Base (KAFB), ECOs, APOs, and Information Technology Asset Users. This supplement applies to individuals at all levels who prepare, manage, review, certify, approve, disseminate and/or use official Air Force Information Technology assets, software, services, and networks, including the Air National Guard (ANG), Air Force Reserve Command (AFRC), and all tenants, satellites, and geographically-separated units, except where noted otherwise. OPR determines no waivers will be granted in this publication. Refer recommended changes and questions about this publication to the OPR using Air Force (AF) Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) AFI 33-322, *Records Management and Information Governance Program*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule. This publication may be supplemented at any level, but all direct Supplements must be routed to the OPR of this publication for coordination prior to certification and approval. 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.

SUMMARY OF CHANGES

This re-write incorporates updates to policy in the following areas: (1) redefining role and responsibilities for tech refresh for laptops and desktop computers, (2) redefining processes related to the IT hardware asset management throughout the asset lifecycle; (3) addresses changes to IT

hardware acquisition due to AFway decommissioning, (4) clarifies roles and responsibilities for conducting inventory of assets while teleworking.

(KIRTLANDAFB) This document has been substantially revised to incorporate changes from the release of the current DAFMAN. Major changes include defined roles, and responsibilities for ECO, Unit Equipment Control Officer (UECO), tenant APO, UAPO, PC and IT users.

Chapter 1

INFORMATION TECHNOLOGY ASSET MANAGEMENT

1.1. General Overview.

1.1.1. This DAFMAN provides guidance and direction for operational management of IT hardware and software assets. It also defines specific roles, responsibilities, and processes within information technology asset management.

1.1.2. Information Technology Asset Management (ITAM) is defined as a framework and set of processes, policies and material solutions that provide efficiency, legal and contractual licensing compliance, financial accountability, and inventory management for software and hardware. To comply with ITAM requirements outlined in this DAFMAN, 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-0).

1.2. Roles and Responsibilities.

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

1.2.1.1. 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), field commands (FLDCOMs), functional managers, and non-DAF 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, must designate the Accountable Property System of Record (APSR) to support ITAM accountability. (T-0). The current designated APSR for Government Owned/Government Operated (GOGO) IT hardware assets is the Defense Property Accountability System (DPAS). The APSR requirements are further defined in **Attachment 2**.

1.2.1.6. Is designated as the official with the responsibility for executing Enterprise Agreements (EA).

1.2.1.7. Conducts data analysis of all DAF IT monetary spent on IT hardware and software assets and asset utilization.

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

1.2.2.1. SAF/CNZC is the Department of the Air Force (DAF) lead for systems operating under Special Access Program (SAP) guidelines in accordance with AFPD 16-7, *Special Access Programs*; AFI 16-701, *Management, Administration, and Oversight of Special Access Programs*, AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*; AFMAN 17-1303, *Cybersecurity Workforce Improvement Program*. DAF Special Access Programs (SAP) IT hardware assets will not be tracked in DPAS. (T-1).

1.2.2.2. SAF/CNZC is responsible for issuing AF Identification (AFID) numbers for SAP IT systems.

1.2.2.3. DAF IT hardware assets under the control of SAF/CNZC will be tracked in the designated APSR by AFID, or other approved accountable systems of record for accountability of hardware, as designated by SAF/CNZC in coordination with SAF/AAZ. (T-1).

1.2.2.4. Software for SAP systems will be managed through SAP channels. Questions regarding Internal Use Software for SAP systems will be directed to SAF/CNZC. (T-1).

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 DAF lead for systems in DAF Sensitive Compartmented Information Facilities (SCIFs), DAF 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)*, DAFPD 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. DAF IT hardware and software 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 AF/A2/6. (T-1).

1.2.3.3. DAF Chief Intelligence, Surveillance, and Reconnaissance (ISR) Information security officer will evaluate all security issues and concerns before directing how DAF 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 and software assets not tracked in the designated APSR. (T-1).

1.2.3.5. AF/A2/6 must manage physical and virtual total lifecycle assets with an automated asset and licensing management system to comply with the Office of the Director of National Intelligence, *Improving Cybersecurity for the Intelligence Community Information Environment Implementation Plan.* (T-0). This will be accomplished via system configuration, network management, license management, and IT service management tools and processes.

1.2.4. **Assistant Secretary of the Department 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 DAF. (T-1).

1.2.4.2. Executes Service Acquisition Executive (SAE) responsibilities outlined in DODI 5000.02, *Operation of the Adaptive Acquisition Framework*, DODI 5000.82 *Acquisition of Information Technology*, DoDI 5000.75, Business *Systems Requirements and Acquisition,* DAFI 63-144, *Business Capability Requirements, Compliance, and System Acquisition,* and all other applicable DOD policy and guidance for execution of DAF acquisitions. (T-0).

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

1.2.4.4. 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).

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

1.2.4.6. Assigns Program Executive Officers (PEOs) to programs per AFI63-101/20-101, *Integrated Lifecycle Management*.

1.2.4.7. Ensures appropriate protection and cybersecurity measures are applied to IT HW &SW acquisitions in accordance with DODI 5000.83, *Technology and Program Protection to Maintain Technological Advantage*, DODI 5000.90, *Cybersecurity for Acquisition Decision Authorities and Program Managers*, and AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology*.

1.2.5. **Air Combat Command (ACC).**

1.2.5.1. Serves as the DAF lead command and DAF-wide systems manager for assigned Systems. (T-1). As the lead command ACC advocates for multi-command (DAF-wide) systems. Advocacy includes planning and programming for acquisition, installation, training, sustainment, testing, and initial operating capability for new systems. The lead Command has total system oversight. (T-1).

1.2.5.2. Serves as lead for implementation and execution of the DAF ITAM program for IT hardware and software. (T-1).

1.2.5.3. Publishes software entitlements, implementation and ITAM account inventory metrics. (T-1).

1.2.5.4. Manages the DAF Evaluated Products List (EPL) and publishes to the DAF portal for the certified commercial-off-the-shelf (COTS) software products for use on DAF networks. (T-1).

1.2.5.4.1. Establishes evaluation and assurance methods and integrates them in the certification process to assure software in accordance with DODI 5000.83, *Technology and Program Protection to Maintain Technological Advantage*, and DODI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*.

1.2.5.4.2. Provides certification documentation to support Authority to Operate decisions when requested. (T-1).

1.2.5.5. Coordinates with SAF/CN, AF/A2/6, Air Force Materiel Command (AFMC), major commands (MAJCOMs) and field commands (FLDCOMs) 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 Major Commands (MAJCOMs), FLDCOMs, Field Operating Agency (FOA), and Direct Reporting Unit (DRU) requirements for potential DAF enterprise software licenses for COTS software.

1.2.5.8. Recommends candidate software products for potential department-wide or DOD-wide licensing to the applicable AFMC and SAF/AQ designated offices with the responsibility for procurement of enterprise licenses as the purchasing agent.

1.2.5.9. Will serve as the DAF software license manager to review and consolidate the DAF-wide software license inventory. (T-1). MAJCOM/ FLDCOM base inventories include locally owned software and software not yet transferred to an enterprise software license agreement.

1.2.5.10. Must maintain a consolidated list of all enterprise and non-enterprise DAF software, to include software name, vendor, version, user (program/WS/MAJCOM/FLDCOM) and platform, and other required data elements as mandated by DODI 5000.76.

1.2.5.11. Designates a product center as the OPR for managing the DAF Enterprise Software License Program or establishing DOD-wide enterprise software license agreements, when designated, acts as executive agent for establishing DoD-wide enterprise software licenses. (T-1).

1.2.5.12. In coordination with SAF/AQ, develop and implement processes to ensures all COTS license requirements are purchased using approved DAF Enterprise License Agreements (ELAs), Joint Enterprise License Agreements (JELAs), DOD Enterprise Software Initiative (ESI) or other approved DOD/ DAF/intelligence community contract vehicles. (T-0). Processes will include methods for contracting officer engagement when the aforementioned agreements and vehicles cannot be used to meet COTS requirements. (T-1).

1.2.5.13. Ensures review of software license agreement language, including coordination with legal and contracting professionals, as necessary. (T-1).

1.2.5.14. 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. (T-1).

1.2.5.15. Designates a product center as purchasing agent for software licenses to support consolidated and programmatic DAF requirements. (T-1).

1.2.5.16. Manages Air Force Enterprise Software Licenses for COTS computer and network management software. (T-1).

1.2.6. **HQ Cyberspace Capabilities Center (HQ CCC) within Air Combat Command (ACC).**

1.2.6.1. ACC delegated governance to HQ CCC. As such, HQ CCC is designated as Program Manager (PM)/lead for the implementation and execution of the DAF ITAM Program through the DAF ITAM Product Management Office (once established) for hardware and software in coordination with the DAF EIT Governance structure and as outlined in the EIT Governance Charter. **(T-1).**

1.2.6.2. Surveys and consolidates MAJCOM/Field Command, FOA, and DRU requirements for potential Air Force enterprise software licenses for COTS computer and network management software.

1.2.6.3. Hosts the following boards to support ACC's lead command responsibilities:

1.2.6.3.1. Service Request Review Board (SRRB).

1.2.6.3.2. Service Design Review Board (SDRB).

1.2.6.3.3. Service Release and Deployment Board (SRDB).

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

1.2.6.5. Reviews request for waivers to this instruction and recommends appropriate actions.

1.2.6.6. Advocates for manpower standards, development and specialty utilization.

1.2.6.7. Assesses equipment, systems and software requirements as directed or requested.

1.2.6.8. Recommends candidate software products for potential DAF-wide licensing to the SAF/CN through the Application Decision Domain Lead and the Service Request Review Board (SRRB).

1.2.6.9. Consolidates new MAJCOM/Field Command training for managing software licenses (including computer-based initiatives) and sends them to Headquarters Air Education and Training Command for incorporating formal courses or in long-distance learning approaches.

1.2.6.10. Provides guidance and support to MAJCOMs/Field Commands, FOAs, and DRUs in managing DAF EIT hardware and software assets.

1.2.6.11. Acts as DAF ITAM functional manager for all proposed upgrades and/or modifications to DAF EIT hardware and software assets.

1.2.6.12. Must maintain the master list of designated Major Command Equipment Control Officers (MECOs) and Base/Tenant IT Equipment Control Officers (ECOs). (T-1).

1.2.6.13. Must manage associated accounts for MECOs and ECOs, to include approving new account requests and conduct annual review of open accounts. (T-1).

1.2.6.14. Must ensure that primary Accountable Property Officers (APOs) for software asset management are appointed in writing and retain appointment letters on file. (T-1).

1.2.6.15. Must act as the Information Owner (IO) for DPAS software and hardware sites, grants DPAS access to all relevant stakeholders (APOs, ECOs, PAs, BSLMs), monitor new access request and conduct annual review of open accounts. (T-1).

1.2.6.16. Must maintain the master distribution list of all appointed software roles (APOs, BSLMs, USLMs, and PA) and has the list readily available. (T-1).

1.2.6.17. Will monitor compliance with annual capital inventory requirements and escalate non-compliance to the Wing Commander. (T-1).

1.2.6.18. Will identify, review, approve, and conduct formal training for all relevant stakeholders for software and hardware asset management. (T-1).

1.2.7. **Air Force Sustainment Center Contracting (AFSC/PZ) - 771st Enterprise Sourcing Squadron**

1.2.7.1. The Air Force Sustainment Center Contracting (AFSC/PZ) will support DAF ITAM Managers and their teams in execution of assigned responsibilities by:

1.2.7.1.1. Conducting Opportunity Assessments. (T-1).

1.2.7.1.2. Supporting the ITAM Program through the ITAM Category Execution Plan (CEP) and in support of the CCC as the lead for the implementation and execution of the DAF ITAM Program for hardware and software. (T-1).

1.2.7.1.3. Executing acquisition solutions across the Category 1, Category Management category. (T-1).

1.2.8. **Service Portfolio Managers (SPM).** The Air Force provides IT through four mission area portfolios: Business, Warfighting, Defense Intelligence, and Information Environment. EIT provides common IT resources, services, hardware, and software segmented into the following sub-portfolios: Protect, Connect, Compute/Store, Enterprise Services, and End User Devices per AFI 17-110, *Information Technology Portfolio Management and Capital Planning and Investment Control*, dated 23 May 2018.

1.2.8.1. Portfolio Owners currently consist of Headquarters Air Force, MAJCOM, USSF, and certain Combatant Command staffs that have DAF IT investments with IEMA sub-portfolios overseen and managed by SAF/CNS. Portfolio Owners will:

1.2.8.2. Be appointed by SAF/CNS as per the EIT Governance Structure and lead assigned Portfolio Managers (PfMs) and/or Category Leads activities on a daily basis. (T-1).

1.2.8.3. Lead Decision Domain/Portfolio members to prioritize at the enterprise-level based on the portfolio roadmap priorities, operational and executability assessments, and trade-off analysis. (T-1).

1.2.8.4. Posture the IT Category Manager and Council Director for the Quarterly DAF Category Management Council. (T-1).

1.2.8.5. Maintain a 12-month forecast of requirements for the Department of the Air Force to buy smarter and more like a single enterprise for all programs in their portfolio. (T-1).

1.2.8.6. Recommend Portfolio Manager/Category Lead assignments (may be the same person) to the SAF/CNS and IT Category Council Director. (T-1).

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 or automated 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 DAF are captured within the general ledger and reported on the financial statements.

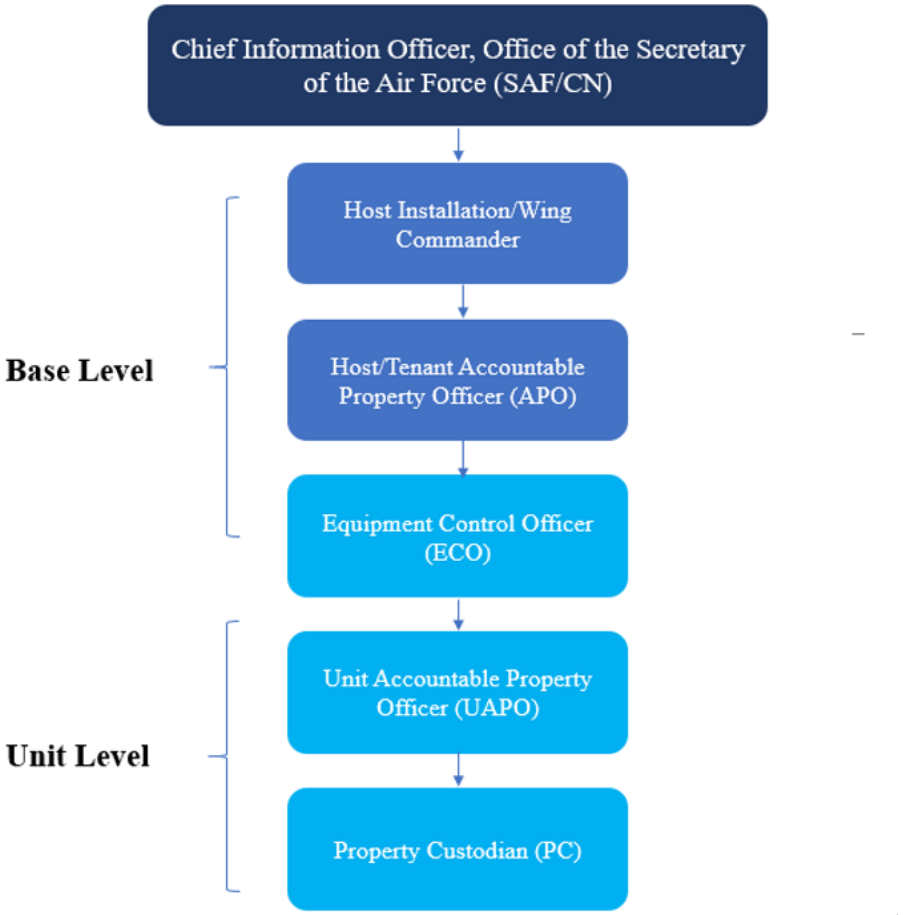
2.2. IT Hardware Definition and Types.

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, 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 a software and firmware. Software and firmware are covered within **Chapter 3**.

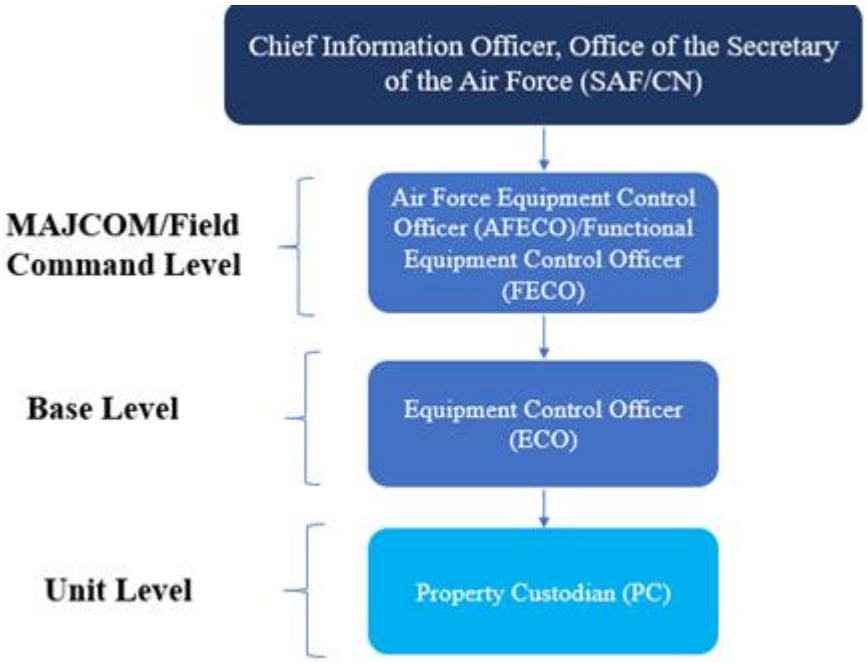
2.3. Roles and Responsibilities. **Figure 2.1** and **Figure 2.2** represent an overview of those hardware asset management roles and responsibilities from the DAF to the organizational level.

Figure 2.1. Property (Physical) Accountability Roles Overview.



Note: The APO role in DPAS is not the same as the host/tenant APO or Unit Accountable Property Officer (UAPO) level. The host/tenant APO and UAPO do not require DPAS access or training.

Figure 2.2. Asset (Financial) Reporting Roles Overview.



2.3.1. **Department of the Air Force Equipment Control Office (DAFECO).**

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

2.3.1.2. Provides guidance and support to MAJCOMs, FLDCOMs, 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/CNS.

2.3.1.4. Coordinates with SAF/CNS 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 ECOs.

2.3.1.7. Manages the implementation of DOD and DAF 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/CNS of required appointments.

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

2.3.1.10. Ensures compliance with this DAFMAN.

2.3.1.11. Resolves compliance issues that cannot be resolved at the host/tenant APO level.

2.3.1.12. Provides reports to MAJCOM/FLDCOM A6s or MAJCOM/FLDCOM inspection teams when requested.

2.3.1.13. 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 (CAGE) code combination. Note: CAGE code is available via: **https://cage.dla.mil/Home/UsageAgree**.

2.3.2. **Functional Equipment Control Officer (FECO).**

2.3.2.1. Serves as the liaison between the DAFECO and ECO.

2.3.2.2. 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, *Enterprise Risk Management and Managers' Internal Control Program Procedures*. (T-0).

2.3.2.3. FECOs may be appointed for FOAs or DRUs where geographical separation from units and high rates of turnover requires an extra tier of oversight for IT Asset Management. The DAFECO will approve FECO appointment requests for FOAs and DRUs. (T-1).

2.3.2.4. FECOs must be appointed in writing by FOA or DRU commander or equivalent with handwritten or digital signatures and provide a digital copy to the DAFECO. (T-1).

2.3.2.5. Completes additional training as directed by the DAFECO.

2.3.2.6. Answers inquiries for ECOs within their area of responsibility.

2.3.2.7. Will review System Authorization Requests (SARs) from their respective ECOs prior to submission to DAFECO. (T-1).

2.3.2.8. Will track appointment of ECOs within their area of responsibility. (T-1).

2.3.2.9. Will ensure ECOs are trained. (T-1). References for ECO training can be found on the DAFECO SharePoint site.

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

2.3.3.1. Must appoint the host APO and maintains appointment letters on file. (T-1).

2.3.3.2. Must appoint tenant APOs in the host tenant support agreement (HTSA), as necessary. (T-1).

2.3.4. **Host/Tenant Accountable Property Officer (APO).**

2.3.4.1. Must be appointed by the host installation commander, wing commander (or equivalent). (T-1).

2.3.4.1.1. **(Added-KIRTLANDAFB)** The Host APO for KAFB will be the 377 Mission Support Group/Communication Division (377 MSG/SC) Commander/Director.

2.3.4.1.2. **(Added-KIRTLANDAFB)** A Tenant APO is any primary or subordinate command of the Regular Air Force, The United States Space Force, The Air National Guard, and the Air Force Reserve, who has not requested Host APO management services in their HTSA.

2.3.4.1.2.1. **(Added-KIRTLANDAFB)** A Tenant APO is responsible for submitting appointment letters to the host Installation Commander for signature.

2.3.4.1.2.2. **(Added-KIRTLANDAFB)** Tenant APOs are responsible for the creation and management of their own Accountable Unit Identification Code (AUIC), appointment of any ECO, as well as the accountability, and disposition of any unit excess assets.

2.3.4.1.3. **(Added-KIRTLANDAFB)** A Tenant who has requested asset management services from the Host APO will be considered a UAPO under the base AUIC. Those tenants have the same responsibilities IAW paragraph 2.3.6..

2.3.4.2. The host APO must be accountable for all accountable IT assets on their installation, unless otherwise delegated in an HTSA. (T-1). The tenant APO will serve as the accountable officer for all accountable IT hardware within their organization. (T-1).

2.3.4.3. 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 DAFECO/FECO. (T-1).

2.3.4.3.1. **(Added-KIRTLANDAFB)** The Host APO may appoint a UECO to provide direct support of tenant units under the host. The Host APO may authorize direct shipments of accountable IT assets to UECO locations. The Host APO may revoke UECO permissions for failure to comply with DoD, AF, or local direction, policy, or guidance.

2.3.4.3.2. **(Added-KIRTLANDAFB)** UECO accounts may be inspected annually by the host base to ensure compliance IAW local, and Air Force Instructions, Manuals, and Policies, regarding IT accountability.

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

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

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

2.3.4.7. **(Added-KIRTLANDAFB)** All Tenant APOs, and UAPOs, will adhere to all IT, Telephonic, Radio, and Software standardization guidance, and approval procedures, as defined by the Host Installation Commander. This includes all mission partners unless specifically granted an HTSA exemption, (T-3).

2.3.4.8. **(Added-KIRTLANDAFB)** Tenant APOs, and UAPOs, will identify their IT requirements IAW **paragraph 2.5.2.6**.

2.3.5. **Equipment Control Officer (ECO).**

2.3.5.1. Must be appointed as primary or alternate by the host/tenant APO. (T-1).

2.3.5.1.1. The Primary ECO will be, at a minimum, the rank of E-5 or GS-7. (T-1). There is not a rank/grade minimum requirement for alternate ECOs.

2.3.5.1.2. Shall only be appointed as a property custodian (PC) for holding assets prior to distribution or disposal (e.g., holding accounts). (T-1).

2.3.5.1.3. Must not be 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).

2.3.5.1.4. If contractor employees are assigned to perform ECO duties under the terms of a contract, the DAF will retain responsibility for determining which supplies and services to purchase. Contractor employees may be authorized to make purchases on the Government's behalf in accordance with Federal Acquisition Regulation (FAR) 7.503(12)(i). Consult with the cognizant Contracting Officer to ensure compliance with contract terms and conditions. (T-1).

2.3.5.1.5. Will track appointment of PCs. (T-1).

2.3.5.1.5.1. **(Added-KIRTLANDAFB)** Will ensure appointment letters are updated in conjunction with a PCs annual account inventory.

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

2.3.5.2.1. Will assist PC in determining the ownership, reassignment, or disposition of all found-on-base accountable IT assets. (T-1).

2.3.5.2.2. Will direct PCs to conduct inventories in accordance with **Attachment 4**. (T-1).

2.3.5.2.2.1. **(Added-KIRTLANDAFB)** May authorize out of cycle inventories.

2.3.5.2.3. Will provide PCs with labels for assets in accordance with **paragraph 2.6.1.4** (T-1).

2.3.5.2.4. **(Added-KIRTLANDAFB)** Contractor operated ECO facilities may physically receive, and store, IT assets pending final receipt and acceptance by government personnel.

2.3.5.2.4.1. **(Added-KIRTLANDAFB)** ECOs may reject damaged shipments entirely, or in part. The ECO must attempt to contact the customer/purchasing officer prior to rejecting any equipment. The ECO may only reject a shipment if the customer has agreed on the return, or they cannot be reached.

2.3.5.2.4.2. **(Added-KIRTLANDAFB)** ECOs will not coordinate vendor returns, or replacements on missing, or damaged deliveries. Those duties are the responsibility of a PC.

2.3.5.3. Will monitor and subscribe to DAFECO SharePoint site for additional guidance and support. (T-1).

2.3.5.4. Will complete additional training as directed by the DAFECO/FECO. (T-1).

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

2.3.5.5.1. **(Added-KIRTLANDAFB)** Training must be provided to PCs annually. Training may be live, virtual, or web based.

2.3.5.6. Will provide inventory assistance in accordance with **Attachment 4**. (T-1).

2.3.5.7. Will ensure on hand serviceable spares for desktops and laptops 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).

2.3.5.8. **(Added-KIRTLANDAFB)** Will review requests for IT resources to determine re-usability of any available bench stock assets and will be the approving authority for reutilization of such assets.

2.3.5.9. **(Added-KIRTLANDAFB)** Will provide a monthly report of account deficiencies to the contract Quality Assurance Representative (QAR).

2.3.5.10. **(Added-KIRTLANDAFB)** Will receive, label, and issue all Defense Property Accountability System (DPAS) accountable IT assets.

2.3.5.11. **(Added-KIRTLANDAFB)** May receive, and issue, non-accountable IT assets.

2.3.5.12. **(Added-KIRTLANDAFB)** Will receive, and process, all DPAS accountable, unclassified, excess IT assets.

2.3.5.12.1. **(Added-KIRTLANDAFB)** Downgraded classified IT assets must have all classification markings removed by a PC before accepting delivery.

2.3.5.13. **(Added-KIRTLANDAFB)** Will receive, and process unclassified non-accountable excess IT assets.

2.3.5.14. **(Added-KIRTLANDAFB)** Will not accept or process classified systems, drives, or media, unless properly equipped, and officially authorized, to do so.

2.3.5.15. **(Added-KIRTLANDAFB)** Will palletize, shrink-wrap, and coordinate disposal of ECO controlled excess with the regional DLA.

2.3.5.16. **(Added-KIRTLANDAFB) Base Equipment Control Officers (BECOs).**

2.3.5.16.1. **(Added-KIRTLANDAFB)** Are appointed by the Host APO, and are the primary installation ECOs subordinate to the 377MSG/SC.

2.3.5.16.2. **(Added-KIRTLANDAFB)** Will provide curbside delivery services of new, and bench stock pulled, DPAS accountable IT assets to 377 Air Base Wing (377 ABW), and subordinate unit property accounts only.

2.3.5.16.2.1. **(Added-KIRTLANDAFB)** Non-accountable assets shipped to an ECO facility will be picked up by the purchasing unit. However, an ECO that has scheduled delivery of accountable assets, may include non-accountable assets in the same delivery.

2.3.5.16.3. **(Added-KIRTLANDAFB)** Will provide curbside pick-up and process all excess IT hardware from 377 ABW, and subordinate unit property accounts only. This includes both accountable and nonaccountable assets.

2.3.5.16.4. **(Added-KIRTLANDAFB)** Will update and maintain the base Automated Data Processing and Equipment (ADPE) website.

2.3.5.16.5. **(Added-KIRTLANDAFB)** Will maintain a government provided bench stock of IT assets, parts, and toner supplies.

2.3.5.16.6. **(Added-KIRTLANDAFB)** Coordinates Site Asset Visits (SAVs) biannually for all accounts not managed by a UECO. SAV's are voluntary and must be accepted by the account PC. An accepted SAV helps to ensure compliance with Air Force Instructions, Manuals, and Policies, regarding IT accountability, and to ensure serviceable spares do not exceed 5%. A written summary of findings will be provided to the PC and a copy retained in the unit account folder.

2.3.5.17. **(Added-KIRTLANDAFB) Unit Equipment Control Officer (UECO).**

2.3.5.17.1. **(Added-KIRTLANDAFB)** Are appointed by the Host APO.

2.3.5.17.2. **(Added-KIRTLANDAFB)** Will Comply with all ECO, requirements, processes, and guidance.

2.3.5.17.3. **(Added-KIRTLANDAFB)** Will manage, update, and track, their own organizational property accounts, and requirements. Records will be kept IAW the BECO file structure referenced in **Attachment 2**, unless granted an exemption by a BECO. Exemptions must be in writing. If automated systems are used, the file structure tab will reference the location of the records (i.e., ServiceNow for 578/1297 records).

2.3.5.17.4. **(Added-KIRTLANDAFB)** Will ensure all Key Supporting Documents (KSDs) for their accounts are uploaded into DPAS.

2.3.5.17.5. **(Added-KIRTLANDAFB)** Will directly receive all new, and excess, IT hardware associated with their unit, if authorized by the Host APO.

2.3.5.17.6. **(Added-KIRTLANDAFB)** Will provide a monthly account deficiency report to the 377th Communications Division Logistics Office (377MSG/SCOL), on the last working day of the month. The report must include the account numbers, and length of time from initial deficiency.

2.3.6. **Unit APO (UAPO).**

2.3.6.1. 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 safeguard IT assets under their control. (T-1).

2.3.6.1.1. **(Added-KIRTLANDAFB)** Any delegation of UAPO duties must be by written appointment. Send appointments letters to the 377MSG/SCOL, ADPE office, or UECO if applicable.

2.3.6.2. 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. (T-0). The UAPO will ensure appointed PCs acknowledge their duties with handwritten or digital signatures, and the UAPO will provide a copy of the documentation to the ECO. (T-2).

2.3.6.2.1. **(Added-KIRTLANDAFB)** Send appointments letters to the 377MSG/SCOL, ADPE office, or UECO if applicable for tenant unit PCs. Appointment letters must include the custodians name, phone number, E-mail, main building number, and Unit Commanders E-mail. Appointment letters are required initially, on appointment, annually with an inventory, or within 30 days of departure of the Unit APO, Alternate APO, or PC.

2.3.6.3. Must be responsible for the accountability of all accountable IT hardware assets assigned to their unit. (T-1).

2.3.6.4. Must approve purchase requests for systems to support mission needs in accordance with **paragraph 2.5** (T-1).

2.3.6.5. Will ensure assets are inventoried according to **Attachment 4**. (T-1).

2.3.6.6. Will ensure PCs perform out-of-cycle inventories as directed. (T-1).

2.3.6.7. Must direct the primary PC to complete a gain-loss inventory no later than 30 calendar days prior to out processing for primary custodian changeover. (T-1).

2.3.6.8. 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).

2.3.6.9. Will develop physical inventory plans and procedures, schedule physical inventories, and assist in their completion in accordance with **Attachment 4**. (T-0).

2.3.6.10. Will ensure on hand serviceable spares for desktops and laptops 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).

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

2.3.6.11.1. **(Added-KIRTLANDAFB)** Training is required within 30 days of PC appointment and annually in conjunction with the unit's annual inventory.

2.3.6.12. **(Added-KIRTLANDAFB)** Ensure all accountable IT hardware assets are shipped to an ECO controlled facility. A UAPO will not directly receive accountable IT assets identified for inclusion in DPAS.

2.3.6.12.1. **(Added-KIRTLANDAFB)** Is responsible for transporting DPAS accountable assets to an ECO facility if received directly by the unit.

2.3.6.13. **(Added-KIRTLANDAFB)** IT assets not accountable in DPAS will be shipped directly to the unit but may be sent to an ECO facility. Assets shipped to an ECO must be picked up by an appointed PC within 15 working days.

2.3.6.14. **(Added-KIRTLANDAFB)** Will not allow IT assets to be cannibalized, thrown away, or otherwise improperly disposed of. All accountable IT excess must be processed through an ECO.

2.3.6.15. **(Added-KIRTLANDAFB)** Will ensure Host APO managed enterprise assets, such as switches, routers, servers, power units, and backup systems, located in a UAPO controlled facility, are not moved without coordination from the 377MSG/SC.

2.3.6.16. **(Added-KIRTLANDAFB)** Will ensure all IT requirements are submitted to the 377MSG/SC IAW **paragraph 2.5.2.6**.

2.3.7. **Property Custodian (PC).**

2.3.7.1. UAPO must appoint primary and alternate PC in writing. (T-1). There is no minimum rank requirement for PCs.

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

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

2.3.7.2.2. PCs will ensure individuals receiving accountable assets validate acceptance with signed documentation i.e., AF Form 1297 or locally developed receipt. PC will retain a copy of the signed document. (T-1).

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

2.3.7.4. Will ensure all accountable assets have labels containing serial number, part number, and manufacturer CAGE code affixed prior to being placed in service. (T-1).

2.3.7.5. Will ensure all shipments are sent to the ECO and will notify the ECO of all incoming and outgoing shipments, transfers, donations, or turn-ins of excess assets. (T-1).

2.3.7.5.1. **(Added-KIRTLANDAFB)** Any accountable assets received directly by the unit, must complete a KAFB form 578 listing new assets, an approved KAFB Form 3215, *Communications System Requirements Document (CSRD),* all copies of packing/shipping documents, and any applicable purchase documentation, to an ECO within 5 working days.

2.3.7.6. 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).

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

2.3.7.8. Upon discovery of lost, stolen, damaged, or destroyed assets will perform the following (refer to **paragraph 2.7.2** for further FLI guidance):

2.3.7.8.1. Must notify the ECO and UAPO within 5 business days. (T-1).

2.3.7.8.2. 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 DoDM 5200.01V3_AFMAN 16-1404V3, *Information Security Program: Protection of Classified Information*, and any local procedures. (T-1).

2.3.7.8.3. Will contact the local Financial Liability Investigation (FLI) office within 5 business days to determine if a FLI is required when any assets within the APSR are discovered lost, stolen, damaged, or destroyed. (T-1).

2.3.7.9. Must ensure hard drives are removed from assets prior to turn-in to DLADS and must contact ISSO or Cyber Security Office to obtain sanitization procedures for hard drives. (T-1).

2.3.7.10. **(Added-KIRTLANDAFB)** Will downgrade/declassify all systems, and drives prior to excess turn-in. Will remove all classified markings from downgraded systems and drives.

2.3.7.11. **(Added-KIRTLANDAFB)** Will check and remove all media from internal drive readers.

2.3.7.12. **(Added-KIRTLANDAFB)** Will not move or replace any enterprise asset without approval from the 377MSG/SC.

2.3.7.13. **(Added-KIRTLANDAFB)** Will maintain an electronic record of account activity IAW **Attachment 2**.

2.3.7.13.1. **(Added-KIRTLANDAFB)** PCs who fall under a UECO will follow all record processes authorized for their unit.

2.3.7.14. **(Added-KIRTLANDAFB)** Must be current on their training and annual inventory to pick up, or drop off, new, or excess IT hardware.

2.3.7.15. **(Added-KIRTLANDAFB)** Will complete out-of-cycle inventories when directed by an ECO.

2.3.7.16. **(Added-KIRTLANDAFB)** Will complete all training as directed by an ECO.

2.3.7.17. **(Added-KIRTLANDAFB)** Will not cannibalize, throw away, or otherwise improperly dispose of, IT assets.

2.3.7.18. **(Added-KIRTLANDAFB)** Will submit all IT requirements IAW **paragraph 2.5.2.6**.

2.3.7.19. **(Added-KIRTLANDAFB) IT Asset Users will:**

2.3.7.19.1. **(Added-KIRTLANDAFB)** Not move any IT asset without authorization of the unit APO, or delegated PC.

2.3.7.19.2. **(Added-KIRTLANDAFB)** Not move, or replace enterprise IT assets without coordination and approval from the 377 MSG/SC.

2.3.7.19.3. **(Added-KIRTLANDAFB)** Not connect any government owned IT asset to a base network without coordination, and approval, from their local Client Support Technician (CST), or the base Communications Focal Point (CFP).

2.3.7.19.4. **(Added-KIRTLANDAFB)** Not connect "personal" devices, sensitive or otherwise, to a government owned, or managed, network unless granted exemption by the Wing Cybersecurity Office (WCO).

2.3.7.19.5. **(Added-KIRTLANDAFB)** Not remove any internal system components.

2.3.7.19.6. **(Added-KIRTLANDAFB)** Not take any government owned IT assets off base, or outside of their unit APOs sphere of control, without having a signed Hand Receipt, AF Form 1297, *Temporary Issue Receipt*.

2.3.7.19.6.1. **(Added-KIRTLANDAFB)** Ensure Hand Receipts are signed by the unit APO, or the delegated PC.

2.3.7.19.6.2. **(Added-KIRTLANDAFB)** When requested by the local supervisor, the PC, the unit APO, or an ECO, the user must present any hand receipted assets within 5 business days.

2.3.7.19.7. **(Added-KIRTLANDAFB)** Ensure all IT assets are properly maintained and secure.

2.3.7.19.8. **(Added-KIRTLANDAFB)** Not leave IT assets in unattended vehicles.

2.3.7.19.9. **(Added-KIRTLANDAFB)** Immediately report damage, or theft, of an IT asset to their appointed PC, or unit APO.

2.4. Accountability Rules of IT Hardware Assets.

2.4.1. **Accountability Technique Determination** .

2.4.1.1. Accountability of IT hardware assets resides with 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 DAF IT hardware assets is determined as follows:

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

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

2.4.1.4. Is supported primarily by 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.

2.4.1.4.1. 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).

2.4.1.4.2. 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 or ECO and provided to UAPO, and be available upon request (e.g., audit). (T-0).

2.4.1.5. 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).

2.4.1.6. **(Added-KIRTLANDAFB)** The scope of accountability is not limited to assets directly connected to an Air Force network. Stand-Alone, enclave, contractor operated, and assets connected to privately operated networks are included, (T-3).

2.4.1.7. **(Added-KIRTLANDAFB)** Assets belonging to other agencies, organizations, companies, or individuals, must be clearly marked to identify ownership, (e.g., Army, Navy, Department of Energy (DOE), Non Appropriated Funds (NAF)).

2.4.1.8. **(Added-KIRTLANDAFB)** An accountable IT asset includes all Government Furnished Property/Government Furnished Equipment (GFP/GFE). See Terms section for applicable GFP/GFE scope.

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. (T-1). 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.

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, that are not tracked elsewhere in an approved APSR. (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 that are categorized as Government Furnished Property (GFP) as defined in DODI 5000.64 and meets any of the criteria in **paragraph 2.4.3** or **paragraph 2.4.4** (T-0).

2.4.3.1.6. Core network and data management infrastructure with unit cost of more than $5,000. Core infrastructure are devices that enable management of network services, e.g., servers, routers, switches, and firewalls.

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 kept current and reflect the current status, location, financial information, and condition of the asset until authorized disposition of the property occurs. (T-1). The property records must provide a comprehensive log of suitable key supporting documents (KSDs) for audit. (T-1). They will also be the authoritative source for use in validating the existence of transactions and completeness of an asset. See **Attachment 5** for a list of KSDs.

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

2.4.4.1. An IT asset/item will be accounted for using the AR process if the asset has a unit acquisition cost of less than $5,000 and any of the following criteria applies:

2.4.4.1.1. The asset/item 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. (T-0). Core infrastructure are devices that enable management of network services, e.g., servers, routers, switches, and firewalls.

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 Hardware 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 **paragraph 2.4.4**, the DAF 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. Peripherals and other IT hardware that do not contain persistent storage capabilities and do not exceed $5,000 (e.g., mice, keyboards, monitors, displays, keyboard video mouse (KVM) switches, voice over internet protocol (VOIP) telephones, and video teleconferencing (VTC) devices, fax machines, mobile hotspots and printers that do not contain HDDs). These assets are not required to be tracked in DPAS, but unit APOs may direct PCs to account for these assets with locally developed procedures.

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, DD Form 200, *Financial Liability Investigation of Property Loss*, etc. (T-1).

2.4.7. **IT Hardware Components of a Weapon System or other Similar Capability.**

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

2.4.7.2. The weapon system is not being managed in another APSR in accordance with Attachment 2, per DODI 5000.64_DAFI 23-111, *Accountability and Management of DoD Equipment and Other Accountable Property*, and AFI 21-103, *Equipment Inventory, Status and Utilization Reporting.* (T-1).

2.4.7.3. 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. Before purchasing standard laptop or desktop computers, review the guidance in **Attachment 3**, A.**3.1.1**.

2.5.1.1. Client computing devices shall be purchased using the Client Computing Solutions III (CCS-3) program including products under the Quantum Enterprise Buy (QEB) cycles as well as Rugged Product Buys (RPB) cycles. (T-0). There are two methods for purchasing the CCS-3 authorized products.

2.5.1.2. For orders restricted to GPC and single delivery location orders utilize the GSA AF Advantage portal.

2.5.1.3. Utilize the Direct to Vendor (DTV) method for delivery orders and BPA calls ensuring orders are transmitted to the specified vendor email addresses for acceptance of encrypted emails. (T-0). The following CCS-3 SharePoint site has the specific vendor contact cards for download to use for this purpose: **https://usaf.dps.mil/sites/aficc/afcc/AFICC/771ESS/SitePages/Client-Computing-Solutions-(CCS-3).aspx**

.Note: Refer to **paragraph 2.6.1.2.2**. in the event orders are not shipped directly to ECO.

2.5.1.4. All orders must be approved by the requesting UAPO, and the servicing ECO. (T-1). Organizations must utilize the CCS-3 purchasing program as the primary means of acquiring client computing systems. (T-0). The products offered under CCS-3 meet all requirements listed above except for limited product types where industry does not have a fully compliant product. In those limited cases, those products are acceptable to purchase for mission requirements but should be limited in quantity. (T-0).

2.5.1.5. The Equipment Control Officer (ECO) will ensure the above standards are met prior to all purchases.

2.5.1.6. For further laptop or desktop acquisition information please contact the 771st ESS Enterprise Hardware Commodity Acquisition Programs (Formerly ITCC) Customer Support at **IT.Contract.Flight@us.af.mil**.

2.5.1.7. Research, Development, Test & Evaluation (RDT&E) units will be exempt. (T-1).

2.5.1.7.1. RDT&E procurement of IT products are not destined for office automation use. Due to the nature of the customer-based IT requirements used in Data Centers or Test Enclaves to support specific mission objectives the standard IT products or configurations will not support the mission. The customer driven requirement directed by program offices or specific customers unique to the RDT&E mission must follow the approval process of the unit Information System Security Managers (ISSM) and Program Office Security personnel. (T-1).

2.5.1.7.2. RDT&E units will procure, where applicable, from CCS-3 or GSA 2GIT approved vendors to meet mission demands from sources identified in **paragraph 2.5** to mitigate risk of infiltration of the supply chain by nation states. (T-1).

2.5.1.8. In the event that a mission requirement cannot be met by CCS-3 through the QEB, RPB or the Specialized Product Solicitation (SPS) request for quote process, organizations must obtain a waiver from the MAJCOM A6. (T-1). If approved, then seek the product using the Second-Generation IT (2GIT) buying program using the GSA portal. Products that are not in scope of CCS-3 do not require a waiver before seeking those products through 2GIT. However, the above technical requirements must be met for all products purchased through 2GIT. (T-0).

2.5.1.9. Digital Printing & Imaging (DPI) products including multifunction/single function printers, scanners, and associated consumables shall be purchased using the Product Selection Cycle (PSC) process. There are two methods for purchasing the DPI authorized products.

2.5.1.9.1. For orders restricted to GPC and single delivery location orders utilize the GSA AF Advantage portal. **https://www.gsaadvantage.gov/**.

2.5.1.9.2. Utilize the DTV method for delivery orders and BPA calls ensuring orders are transmitted to the specified vendor email addresses for acceptance of encrypted emails. (T-0). The following DPI SharePoint site has the specific vendor contact cards for download to use for this purpose: **https://usaf.dps.mil/sites/aficc/afcc/AFICC/771ESS/SitePages/Digital-Printing-and-Imaging-(DPI).aspx**.

2.5.1.9.3. For further information please contact customer support at **itccsupport@us.af.mil**.

2.5.1.10. Cellular Services and Devices (CSD) are available through Navy Spiral 3 (current)/Navy Spiral 4 (future) and provide wireless devices and services. **https://my.navsup.navy.mil/apps/ops$ncmpo.view_topic?p_topic_id=TOPIC_144**.

2.5.1.11. GSA 2nd Generation IT (2GIT) provides network Infrastructure hardware and services (servers, routers, switches, etc.), end user devices, and other IT hardware for purchase and should be accessed through GSA Advantage. (T-0). **https://www.gsaadvantage.gov/advantage/ws/department/adv2git**.

2.5.1.12. Other Government-Wide Acquisition Contracts (GWACs) authorized for use.

2.5.1.12.1. The CCS-3 and DPI purchase sources are mandatory and take precedence over GSA 2GIT and other procurement sources, unless waived by the MAJCOM/Field Commands/A6s or equivalent. (T-1). Note: a waiver is not required to use 2GIT if the IT hardware requirement is outside of the scope of CCS-3 and DPI (i.e. network infrastructure requirements such as servers, routers, switches, etc.). (T-0).

2.5.1.12.2. 2GIT is mandatory and takes precedence over other GWACs and other vendor authorized sources, unless waived by the MAJCOM/Field Command/A6s or equivalent/as designated. (T-1).

2.5.1.12.3. All managed print services will be procured using guidance in **paragraph 2.5.3** (T-1).

2.5.1.12.4. All requests for servers must comply with current National Defense Authorization Act (NDAA). (T-0).

2.5.1.13. The minimum hardware specifications, processes and contract vehicles defined in this guidance are current as of February 2022 and subject to change. (T-0). Refer to the 771st ESS Enterprise Hardware Commodity Acquisition Programs (Formerly ITCC) Customer Support at **IT.Contract.Flight@us.af.mil** or **ITCC.Support@us.af.mil** for the latest direction regarding the purchase of IT hardware.

2.5.1.14. **(Added-KIRTLANDAFB)** Requirements for any IT, Telephonic, or Radio assets, solution, service, connection, support, move, or software, must be identified to the 377MSG/SC for review, IAW **paragraph 2.5.2.6** This includes all Tenant APOs, UAPO, and contractors providing support to the Regular Air Force, The United States Space Force, The Air National Guard, and the Air Force Reserve.

2.5.2. **Procurement Process.**

2.5.2.1. ECOs will ensure they provide complete information for shipping labels for ordered equipment. (T-1). 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. **https://www.gsaadvantage.gov/**

2.5.2.1.1. "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).

2.5.2.1.2. "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). For further information please contact customer support at **itccsupport@us.af.mil**.

2.5.2.1.3. Central receiving facilities and warehouses must meet manufacturer operating and storage environment specifications, standard facility requirements and DAF safety standards to protect assets from physical damage and inclement weather. (T-1).

2.5.2.2. All Accountable IT hardware assets must be added to DPAS in accordance with **Attachment 2**. (T-1).

2.5.2.2.1. If an asset is not loaded in the DPAS Catalog, the ECO must submit a catalog update request through the DAFECO SharePoint DPAS Catalog Update Request system. (T-1).

2.5.2.2.2. The manufacturer name, part number, model number and CAGE code must be provided along with documentation (e.g., invoice, shipping document, etc.) and KSD (e.g., packing slip). (T-1).

2.5.2.2.3. IT hardware monetary value for accountable assets as described in **paragraph 2.4.4** must be recorded in DPAS. (T-1). The monetary value of an accountable asset recorded in DPAS shall not include peripheral devices received with the asset. (T-1).

2.5.2.3. Standard Laptop and Desktop Computers will be refreshed per **Attachment 3**. (T-1).

2.5.2.4. End user devices listed in **Table 2.2** may be refreshed at the recommended refresh schedules or when the asset no longer meets operational requirements.

Table 2.1. End User Device Refresh Rate.

Device Type	Recommended
Tablet	4 years
Mobile Devices	2 years
Printer	5 years
Radio	10 years

2.5.2.5. Monitors will only be replaced when unserviceable or when unable to interface with current technology.

2.5.2.6. **(Added-KIRTLANDAFB) KAFB Requirements Process.**

2.5.2.6.1. **(Added-KIRTLANDAFB)** Units will identify their IT requirements using a KAFB Form 3215. CSRDs will be submitted for processing to the 377 MSG/SC at: **3215helpdesk@us.af.mil**.

2.5.2.6.1.1. **(Added-KIRTLANDAFB)** Units must complete all internal reviews prior to submitting a CSRD. Missing signatures may cause a delay or rejection.

2.5.2.6.1.2. **(Added-KIRTLANDAFB)** No unit may purchase, install, or connect IT, Telephonic, Radio devices, without an approved CSRD.

2.5.2.6.1.3. **(Added-KIRTLANDAFB)** No unit may purchase software without an approved CSRD.

2.5.2.6.1.4. **(Added-KIRTLANDAFB)** No unit may move 377MSG/SC managed Enterprise assets, switches, routers, servers, power units, or connections to such, without an approved CSRD.

2.5.2.6.2. **(Added-KIRTLANDAFB)** Telephone requirements must be reviewed, signed, and submitted, by a unit appointed Telephone Control Officer (TCO).

2.5.2.6.2.1. **(Added-KIRTLANDAFB)** TCO appointment letters must be submitted to the 377MSG/SCX office on appointment, annually, and within 30 days of a custodian's departure. Appointment letters must contain the appointee(s), full name, phone number, E-mail address, and account number.

2.5.2.6.3. **(Added-KIRTLANDAFB)** A Unit Software License Manager (USLM) must review all software requirements. The USLM, PC, or UAPO may submit a CSRD.

2.5.2.6.3.1. **(Added-KIRTLANDAFB)** USLM appointment letters must be submitted to the 377MSG/SCXS on appointment, annually, and within 30 days of a custodian's departure, and a copy provided to the 377MSG/SCOL ADPE office.

2.5.2.6.4. **(Added-KIRTLANDAFB)** All other IT requirements must be submitted by an appointed PC.

2.5.2.6.5. **(Added-KIRTLANDAFB)** CSRDs expire 365 days from the date of submission. Expired CSRDs, or CSRDs which have not been executed within the 365-day window, must be resubmitted if the requirement still exists.

2.5.2.6.6. **(Added-KIRTLANDAFB)** A CSRD will be cancelled if a duplicate requirement exists, when a scheduled appointment has been missed, or multiple unsuccessful attempts have been made to contact the submitter.

2.5.2.6.7. **(Added-KIRTLANDAFB)** CSRDs will be rejected if incomplete, are not the correct version, or are not signed by the proper appointed authority. Purchase requests will be rejected if the unit's inventory is delinquent, or the submitting PC has not completed annual training.

2.5.2.6.8. **(Added-KIRTLANDAFB)** Units must resubmit a CSRD if the original approved requirement has changed. Units may be required to resubmit a CSRD at the request of a 377MSG/SC communications officer, or other authorized approver.

2.5.2.6.8.1. **(Added-KIRTLANDAFB)** Quantity changes do not require resubmission.

2.5.2.6.9. **(Added-KIRTLANDAFB)** General information for a CSRD is available on the 377MSG/SC ADPE website, (**https://usaf.dps.mil/sites/10324/ADPE/SitePages/Home.aspx**), or by calling 505-853-3215.

2.5.3. **Managed Print Services (MPS).**

2.5.3.1. 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.

2.5.3.2. MAJCOMs and FLDCOMs 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).

2.5.3.3. New MPS contracts must be procured through either Defense Logistics Agency (DLA) Equipment Management Solutions or General Services Agency (GSA) Schedule 36, 541611MPS. (T-1). Contact local contracting office for guidelines to executing an MPS contract/obtaining print services.

2.5.3.4. MAJCOMs or FLDCOMs will maintain a minimum of a 1:30 printer to user's ratio for each network enclave. Facilities/enclaves with fewer than 30 users will be limited to a single printer. (T-2).

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

2.5.3.6. For compelling, mission-essential operational requirements that cannot be fulfilled through Managed Print Services, DAF organizations must request a waiver by submitting justification through their parent MAJCOM A6 or FLDCOM for exception to guidance. (T-2). Waiver can be found in the DAFECO SharePoint site.

2.6. Receipt and Acceptance of IT Hardware.

2.6.1. Receipt and Acceptance of IT Hardware Assets in DPAS.

2.6.1.1. IT asset accountability must be established by formal receipt and acceptance in DPAS according to DODI 5000.64. (T-0). DAF IT asset accountability will be conducted in a timely manner using the following procedures.

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

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

2.6.1.2.2. If anyone 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)

2.6.1.2.2.1. **(Added-KIRTLANDAFB)** If DPAS accountable assets were shipped to a unit, it is the UAPOs responsibility for ensuing all Key Supporting Documents (KSDs) are provided to an ECO. If those assets require movement to an ECO controlled facility, at the determination of an ECO, the responsibility for loading, transporting, and offloading is the UAPOs.

2.6.1.2.3. If an asset cannot be found in the current DPAS catalog, the ECO will submit a catalog update request through the DAFECO SharePoint site. (T-1).

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

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

2.6.1.4. The ECO will ensure all accountable assets have labels containing serial number, part number and manufacturer CAGE code affixed prior to being placed in service. (T-1).

2.6.1.4.1. When the device is too small labels, a label is not required. (T-1).

2.6.1.4.2. The PC will ensure asset data is accurately loaded to DPAS. (T-1).

2.6.1.5. **(Added-KIRTLANDAFB)** Non DPAS accountable IT assets, internal components, and supplies should be shipped directly to the unit. Assets may be shipped to an ECO facility, but it will be the unit's responsibility to retrieve the assets within 15 business days.

2.6.1.6. **(Added-KIRTLANDAFB)** It is the UAPO, or their appointed PCs, responsibility to coordinate all vendor returns, or assistance for missing products, or repairs. Any replacement of an accountable asset must be shipped to an ECO facility.

2.6.2. **Program 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. (T-1).

2.6.3. **DPAS Structure.**

2.6.3.1. ECOs will align their IT asset accounts within DPAS by using the DAF approved DPAS account structure below. (T-1).

2.6.3.2. ECO will use Accountable Unit Identification Codes (AUIC) to identify the location, multiple Unit Identification Codes (UICs) to identify units, and multiple custodians to identify unit accounts, as per example listed below:

Table 2.2. DPAS Structure Example.

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

2.7. Sustainment of IT Hardware Assets.

2.7.1. **Inventory.**

2.7.1.1. General requirements. The purpose of an inventory is to ensure accountable assets reported on the general ledger and the financial statement exist and can be readily located. Any accountable assets in the possession of the DAF must be accounted for in DPAS in accordance with applicable property and financial management policies and as prescribed in DODI 5000.64. (T-0).

2.7.1.2. Remote or Teleworking assets. IT assets being utilized for remote or telework purposes may be inventoried by the individual assigned the asset. Inventories of remote or teleworking assets will be accomplished in accordance with the **Attachment 4**.

2.7.1.2.1. Assets meeting the accountability criteria for Accountable Property Record and the Accountability Record stated in **paragraph 2.4.3** and **paragraph 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 ®, 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 DAF for the inventory of IT assets can be found in **Attachment 4**.

2.7.2. **Financial Liability Investigation (FLI).**

2.7.2.1. For any loss, damage, theft, or destruction of assets within the APSR, the PC will perform the actions identified in **paragraph 2.3.7.8** to determine if a FLI is required. (T-1).

2.7.2.2. If a FLI is required, the UAPO will follow the FLI procedures provided by the local FLI office. (T-1).

2.7.2.3. If a FLI is not required, the PC will obtain a signed Memorandum for the Record (MFR) from the UAPO stating that a FLI was not required as determined by the local FLI office and removal of the asset from the APSR is approved. (T-1). The PC will provide the UAPO signed copy of the MFR to the ECO. (T-1). The ECO will then adjust the asset record from DPAS and upload the signed MFR as a KSD. (T-1).

2.7.2.4. Contractor Guidance. Establish the extent of contractor liability in the provisions of the applicable contract's government property clause according to DODI 5000.64_DAFI 23-111.

2.7.3. **Managing Capital Assets**

2.7.3.1. The capitalization threshold for capital IT hardware assets is $1,000,000 or greater as prescribed in DOD FMR 7000.14-R, Volume 4, Chapter 25, "General Equipment".

2.7.3.2. IT hardware assets fall under general equipment capital assets and follow the same capitalization criteria as defined by DOD FMR 7000.14-R, Volume 4, Chapter 25.

2.7.3.3. The capital cost for capital IT hardware asset 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) as prescribed in DOD FMR 7000.14-R, Volume 4, Chapter 25.

2.7.3.4. ECOs will review criteria in **paragraph 2.7.3.1** through **paragraph 2.7.3.3** prior to designating IT hardware asset as capital in DPAS.

2.7.3.5. Capital Assets will:

2.7.3.5.1. Have a valid fund code assigned within DPAS. Reference the QRGs available on the DPAS support page and the "DPAS Additional Training and Quick Reference Guides" section within the DAFECO SharePoint for instructions on how to properly create valid fund codes. (T-1). POC for fund codes will be the servicing resource advisor or contracting office.

2.7.3.5.2. Have depreciation activated within DPAS. For additional information, reference the DPAS support page and the "DPAS Additional Training and Quick Reference Guides" section within the DAFECO SharePoint site. (T-1).

2.8. Disposition of IT Hardware Assets.

2.8.1. **Transfers.**

2.8.1.1. 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 DAF. (T-1). ECO must check the designate box in DPAS when transferring an asset. This will ensure the gaining ECO is alerted to the incoming transfer. (T-1).

2.8.1.2. 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.

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

2.8.1.2.1.1. The gaining ECO will acknowledge receipt of transferred assets in DPAS with 7 calendar days of receipt notification. (T-1).

2.8.1.2.2. 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*. (T-1). For local transfers where no shipping activity is involved, the gaining and losing PC must sign the DD Form 1150, *Request for Issue/Transfer/Turn-In*, or locally generated transfer form. (T-1).

2.8.1.2.3. The losing activity ECO:

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

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

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

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

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

2.8.1.2.4.1. Identify and report maintenance contracts that supported transferred assets to contracting officials. (T-1).

2.8.1.2.4.2. Assist contracting officials as required, in transferring contracts to the gaining activity. (T-1).

2.8.1.2.4.3. Review hardware assets release dates. Give adequate notice to the vendor to preclude payment of extra costs. (T-1).

2.8.1.2.4.4. Coordinate hardware assets release dates with other base functions, as required. (T-1).

2.8.1.2.4.5. Ensure hard drive sanitization according to AFMAN 17-1301, *Computer Security (COMPUSEC)*, and National Institute of Standards and Technology, SP 800-88 Rev. 1, Appendix A, Table A1-A9, *Guidelines for Media Sanitization*. (T-1).

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

2.8.1.2.4.7. Properly inventory, package, warehouse, and secure equipment when storing hardware assets before transfer. (T-1).

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, and Lifecycle Support Plan (AS/ LCSP). Reference AFI 63-101/20-101, *Integrated Lifecycle Management* for further information about the AS/ LCSP. According to DODI 5000.64_DAFI 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 will be redistributed to other units as needed. Redistribution will be coordinated between ECOs. Gaining units will be responsible for shipping costs if location is outside the local area. (T-1). If assets cannot be redistributed, they will be condition coded as "F, G, or H" and turned in to DLADS. For further information on DPAS condition codes, see **paragraph A2.2.3.9** (T-1).

2.9.1.3. The PC will notify the ECO when hardware assets is identified as excess no later than 30 calendar days before the equipment goes off-line. 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).

2.9.1.3.1. **(Added-KIRTLANDAFB)** The PC will complete a KAFB Form 578 when excessing accountable IT assets to an ECO or transferring excess assets to another base accounts. Copies of transferred documents must be sent to an ECO.

2.9.1.4. When an organization receives a replacement IT asset for a technical refresh or replaces an unserviceable asset, the ECO will assign the asset being removed with DPAS condition code "F, G, or H", "Ready for turn in", and then contact the local DLADs facility to schedule an appointment for turning in the asset. (T-1).

2.9.1.4.1. 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). Once DLADs has received the asset and completed the turn in, the ECO will remove the asset from the APSR within 30 calendar days. (T-1).

2.9.1.4.2. No further assets of the same type will be purchased by the organization until the assets being replaced have been condition coded as "Ready for turn in" and DLADS has been contacted to schedule turn in. (T-1).

2.9.1.4.3. If DLADs cannot process an asset turn in within 60 calendar days, the ECO will document the scheduled DLADs appointment in the history remarks section for the asset in DPAS.

2.9.1.5. Dispose of and/or reuse classified media and systems according to the guidance in **paragraph 2.10.3**.

2.9.1.6. Per FAR 7.503©(11), ensure that disposal is performed by government personnel only, unless a specific authority is given to the contractor to dispose of property at prices within specified ranges and subject to reasonable conditions as deemed appropriate by the DAF. (T-0).

2.9.1.7. **(Added-KIRTLANDAFB)** No unit or individual may cannibalize assets without authorization from an ECO.

2.9.1.7.1. **(Added-KIRTLANDAFB)** Removal of hard drives does not constitute cannibalization. Hard drives may be retained, reutilized, given to an ECO, or destroyed by the unit.

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 or FLDCOM.

2.9.2.2. Excess hardware may be transferred from AUIC to AUIC 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. Host bases utilizing a regional DLADS facility may be required to establish a MOA. When necessary, 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, Volume 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 17-1301, National Institute of Standards and Technology, *Guidelines for Media Sanitization*, SP 800-88, Appendix A, and Manual 9-12, *Storage Device Sanitization and Destruction Manual*. (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. Accountable DAF 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 appointed ECO or PC may turn in equipment to DLADS when necessary, e.g., disposal, turn-in, etc.

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

Chapter 3

SOFTWARE ASSET MANAGEMENT

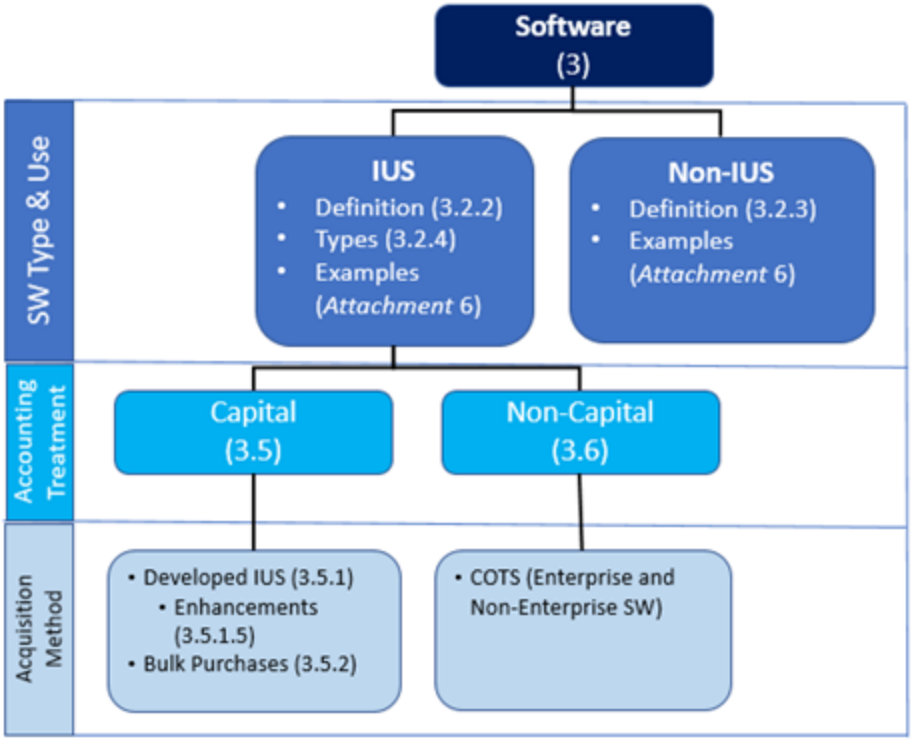
3.1. Overview and Scope.

3.1.1. This chapter provides guidance for physical and financial accountability and management of Department of the DAF software. 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. The requirements for this chapter are derived from the following overarching DoD policies: SFFAS 10, DODI 5000.76, and DoD FMR, volume 4, chapter 27.

3.1.2. Software asset management shall be centralized and managed at the highest level of common usage. As the designated Program Manager (PM)/lead for the implementation and execution of the DAF ITAM Program, HQ CCC will work with ESLMs, BSLMs, APOs and SBAs to centralize and govern software asset management for DAF. (T-1). The Commander (or equivalent) at each installation shall implements licensed COTS or other software for local requirements not fulfilled by enterprise software licensing. The management of software licenses at the base level does not include those software licenses that are managed through enterprise software licensing programs. Software asset management program ensures organizations that deploy and manage COTS software track software entitlements and implementation information.

3.1.3. This chapter excludes guidance for software that is not IUS (non-IUS). Examples of non-IUS software are embedded software (firmware), 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 for as part of the equipment in which it is installed. For a comprehensive list of IUS and non-IUS assets, refer to **Attachment 6**. Refer to **Figure 3.1** for software guidance organized by software type, accounting treatment, and acquisition method definitions and cross-references to governing paragraph in this publication.

Figure 3.1. Software Guidance Breakdown.



3.2. Software Definition and Types.

3.2.1. **Software Definition.**

3.2.1.1. Per Statement of Federal Financial Accounting Standards (SFFAS) 10: *Accounting for Internal Use Software*, software includes 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. Is acquired or developed to meet internal or operational needs.

3.2.2.3. Is used to operate DAF 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).

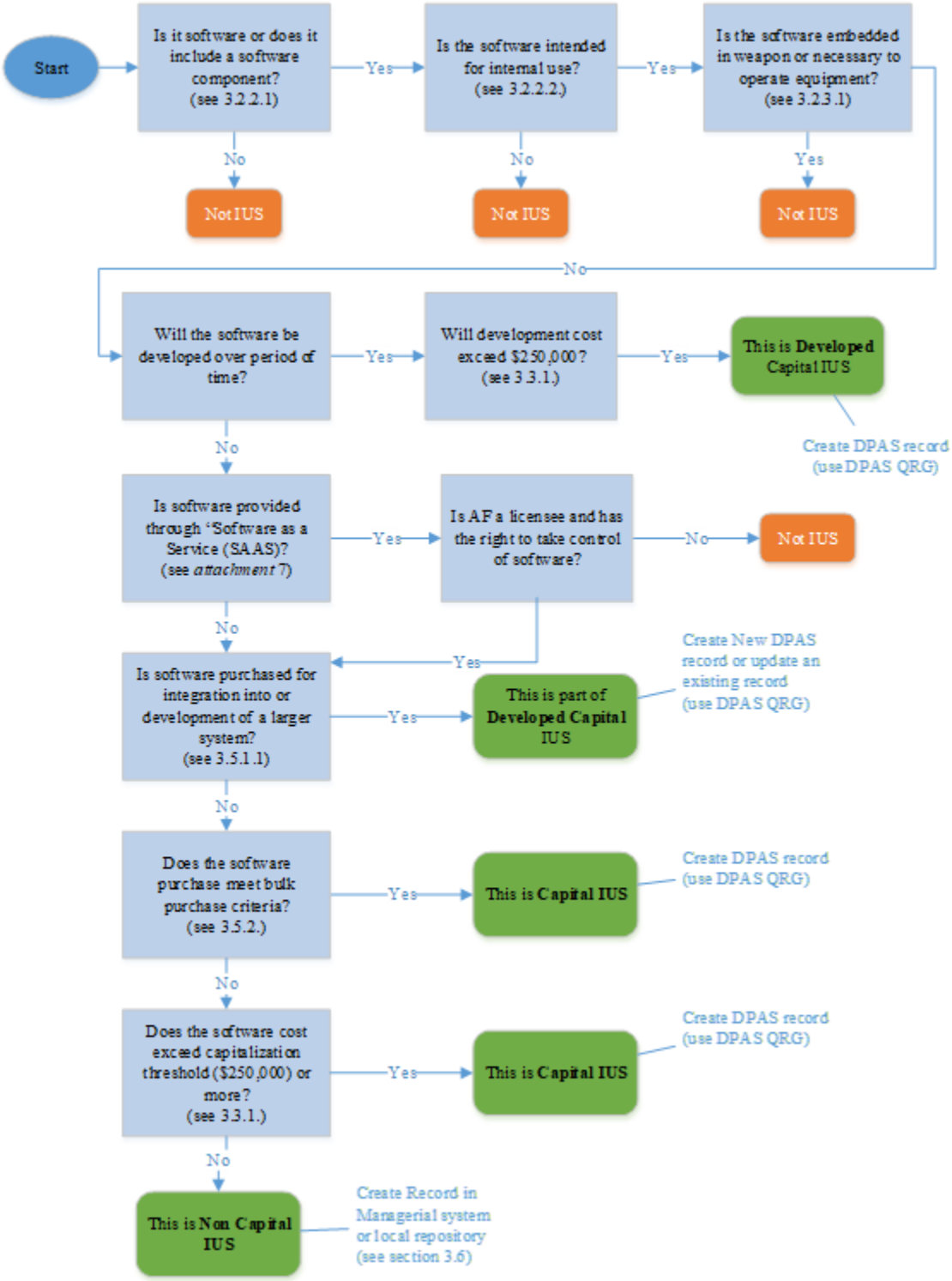
3.2.3. **Non-IUS.**

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.



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 acquired from a vendor and is 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 DAF 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 (DAF personnel) for which it is created.

3.2.4.3. For additional examples of IUS, please see Attachment 6.

3.3. Internal Use Software Financial Criteria.

3.3.1. **Capital 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.

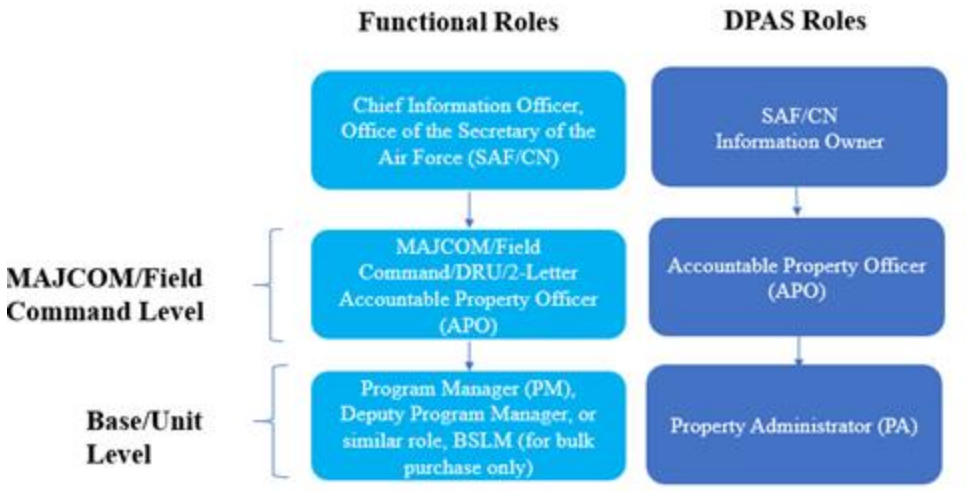
3.3.1.4. Additional capitalization criteria related to software licenses purchased in bulk and enhancements to the existing software is outlined in **paragraph 3.5** of this guidance.

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 (IUS) Roles.



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

3.4.1.1.1. Serves as APO for all capital IUS assets owned by their MAJCOM/2-Letter organization and must be appointed by the MAJCOM commander or equivalent. (T-1). HQ CCC will oversee the appointment of the role and will retain appointment letters on file.

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. May delegate duties to additional APO to enable execution but the ultimate responsibility for execution will remain with the APO. (T-1).

3.4.1.1.4. Is responsible for establishing UICs for their specific AUIC, train alternative APOs, and update key data elements within the DPAS that are beyond the scope of PA or CM role (e.g., Asset ID Prefix, Fund Code, Document Number range).

3.4.1.1.5. Must maintain the authoritative list of all capital IUS owned by the organization and be able to provide the list upon request within 7 days. (T-1).

3.4.1.1.6. Must appoint in writing, DPAS Property Administrator (PA), Base Software License Manager (BSLM), and DPAS PA. (T-1). Must retain appointment letter on file and provide a copy to SAF/CN, ACC/A6, CCC and AFMC/A6/Managed Services Office (MSO), if requested. (T-1).

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

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

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

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

3.4.1.2. **DPAS Software Catalog Manager (CM).**

3.4.1.2.1. HQ CCC will oversee the appointment and execution of this role and will retain appointment letters on file. (T-1).

3.4.1.2.2. DPAS Catalog Manager will oversee the standardization of software catalog in DPAS and will be responsible for creating and maintaining software catalog entries for all capital software across DAF. (T-1).

3.4.1.2.3. Must work closely with MAJCOM/FLDCOM/DRU/2-Letter APO, DPAS PA, BSLMs, and ESLMs to establish software catalog items in a standardized and consistent manner. (T-1).

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

3.4.1.3. **DPAS Property Administrator (PA).**

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

3.4.1.3.2. It could 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. (T-1).

3.4.1.3.3. Must work closely with DPAS CM to establish new catalog items for capital IUS, if IUS asset cannot be found in the current DPAS catalog. (T-1).

3.4.1.3.4. Must work closely with the PM, CO, CO representative or COR equivalent to ensure contracts related to acquisition of developed IUS, included CLIN structure detailed in **Table 3.1** (T-1).

3.4.1.3.5. Must collect and maintain 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).

3.4.1.3.6. 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).

3.4.1.3.7. Must track and enter valid major IUS enhancement cost data; retain documentation related to IUS enhancement decisions (e.g., 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).

3.4.1.3.8. Must notify DPAS APO of all IUS changes in capital IUS life-cycle events (e.g., 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).

3.4.1.3.9. Must take DPAS PA level training and obtain access to DPAS FF-CIOGE site. (T-1).

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

3.4.1.4. **Base Software License Manager (BSLM) DPAS PA.**

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

3.4.1.4.2. Non-capital IUS management responsibilities for this role are outlined in **paragraph 3.4.2.6**.

3.4.1.4.3. Capital IUS responsibilities for this role include:

3.4.1.4.3.1. Must establish asset accountability record in DPAS for IUS that meets capitalization criteria as prescribed in **paragraph 3.3.1** of this guidance. (T-1).

3.4.1.4.3.2. 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).

3.4.1.4.3.3. Must maintain accountability records in DPAS and notify MAJCOM/FLDCOM /DRU/2-letter DPAS APO if changes in the lifecycle of the asset record occur. (T-1).

3.4.1.4.3.4. Must assist MAJCOM/FLDCOM/DRU/2-letter DPAS APO with annual capital software asset inventory. (T-1).

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

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

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

3.4.1.5. **Contracting Officer (CO).**

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

3.4.1.5.2. 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).

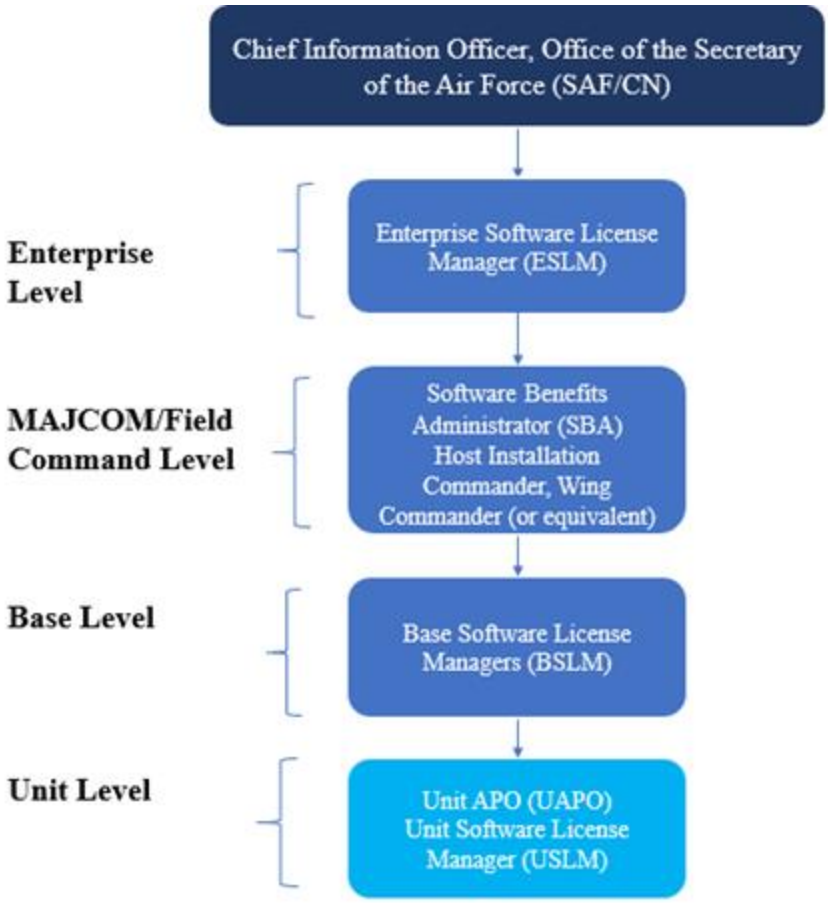
3.4.1.6. **Contracting Officer Representative or equivalent.**

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

3.4.1.6.2. Notifies the CO when CLIN or CDRL content is invalid or missing.

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 DAF to the organizational level.

Figure 3.4. Non-Capital IUS Physical Accountability Roles.



3.4.2.1. **Enterprise Software License Manager (ESLM).**

3.4.2.1.1. This role shall be located at HQ CCC. ESLM serves as the DAF-wide software requirements manager for JELAs and other DAF-wide licensing agreements, to include support of Combatant Commands for whom the DAF is the Executive Agent.

3.4.2.1.2. Must consolidate and analyze software inventories to support JELA reporting requirements and ensure compliance with ELA requirements concerning appropriate availability, distribution and usage of the subject software. (T-1).

3.4.2.1.3. Must validates requirement approved by MAJCOM/ FLDCOM Software Benefits Administrators (SBAs) and submits price quote requests to the JELA vendor. (T-1).

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

3.4.2.2. **MAJCOM, FLDCOMs, DRU, FOA, or Equivalent.**

3.4.2.2.1. Appoints in writing, an APO, SBA, and BSLM. Must sign the appointment letter and document acknowledgement of duties with handwritten or digital signatures. The appointment letter will be retained by HQ CCC.

3.4.2.3. **Software Benefits Administrator (SBA).**

3.4.2.3.1. This is a MAJCOM, FLDCOMs, DRU, or 2-letter role.

3.4.2.3.2. Ensures all COTS software products are purchased using approved DOD/DAF Enterprise Licenses Agreements (ELAs), DOD ESI or approved DOD/ DAF contract vehicles. (T-1). For SCI and ISR requirements, ensure IC ELAs and IC enterprise contract vehicles are used. (T-1).

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 appoint 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).**

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

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

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

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

3.4.2.5.5. 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/ or FLDCOM and service owner for Enterprise IT. (T-2).

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

3.4.2.6. **Base Software License Managers (BSLMs).**

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 3.4.1.4** 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 KSDs 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 an annual inventory of enterprise software licenses. The annual inventory will include reconciling licenses against contract information in order 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/ DAF /IC ELAs, DOD ESI or approved DOD/ DAF/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.

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. (T-1). 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 or BSLM. (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). The enterprise and non-enterprise inventories may be combined into a single inventory using available tools.

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 retains 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 7000.14-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, assembles proofs-of-purchase, and requests 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 submits 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. Can be a contractor, government civilian or military member.

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

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

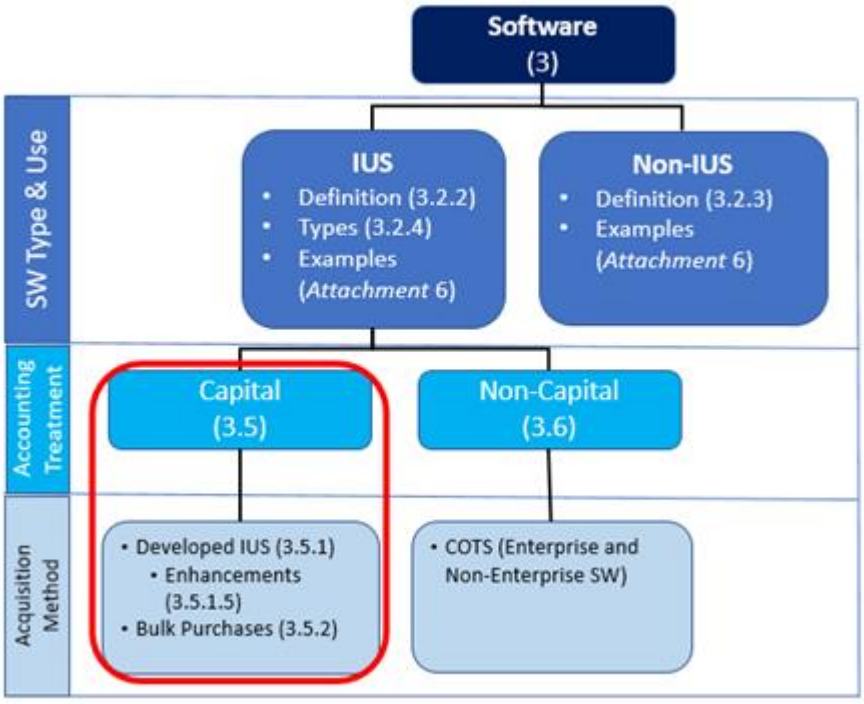
3.4.2.9.2. Notifies USLM (or equivalents) of any actions performed that changes local software licenses installed on computer systems. Must maintain a record of and notify USLMs when installing software from shared folders or using installation CDs/DVDs. (T-3). Also maintains a record of and notifies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

3.4.2.9.3. Ensures that only software listed on the DAF Evaluated Products List (EPL), is installed, in accordance with AFI 17-130, *Cybersecurity Program Management*.

3.4.2.9.4. Ensures that reciprocity requirements are followed in accordance with AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*.

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 DAF, including new software that is modified with or without a contractor's assistance; or contractor-developed software that DAF 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 the process for capturing labor cost for software that was developed or modified by DAF 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 Contracting Officer (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, DAF 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. (T-1).

3.5.1.2.7. Ensure contracts for the development of IUS include a listing of all contractor- supplied IUS. (T-1).

3.5.1.2.8. Ensure the requiring activity has included a discussion the types and approximate quantities of IUS required in the acquisition plans, strategy documents, and requirements packages. (T-1).

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. Ensure invoices contain the contract line-item level detail for all firm fixed price contracts that are not administered by the Defense Contract Management Agency (DCMA). (T-1).

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 CM 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 receipt of vendor invoices, the PMO/COR will validate that the invoices conform to the terms of the contract regarding developed IUS CLIN and CDRL identifications. (T-2). The COR will do the following in determining whether to approve or reject invoice in the Wide Area Workflow (WAWF) module in the Procurement Integrated Enterprise Environment (PIEE). (T-2):

3.5.1.3.2.1. Ensure that CDRL information, as defined during contracting activities is reported by the vendor. (T-2).

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

3.5.1.3.3. 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).

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

3.5.1.3.5. 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).

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

3.5.1.3.7. AF Form 7500 might include:

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

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

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

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

3.5.1.3.8.4. 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).

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

3.5.1.3.9.1. 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.

3.5.1.3.9.2. Training costs: post-deployment training costs.

3.5.1.3.9.3. 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).

3.5.1.3.9.4. 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 manual.

3.5.1.3.10. 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. (T-0).

3.5.1.3.11. MDA will determine 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).

3.5.1.3.12. PM/FO will obtain the 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, the PM will provide the DDM to DPAS PA. (T-2).

3.5.1.3.13. 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).

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

3.5.1.3.15. Please refer to **Figure A7.1** for the 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 enhancement types will be capitalized by the DAF. (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, paragraph 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 likely 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 3.5.1.5** 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 DAF. (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. Accountable organizations must adhere to product licensing agreements when transferring, disposing, or reusing commercial IUS in order 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 the process 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 3.6.3**.

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** 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 (do not include software maintenance cost in 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 the terms of the license agreement. (T-1): Methods that may comply with license agreement terms include:

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

3.5.2.4.1.2. Destroy the software and license keys according to the provisions of the licensing agreement. (T-1):

3.5.2.4.1.3. Document the method of destruction to establish an audit trail. (T-1):

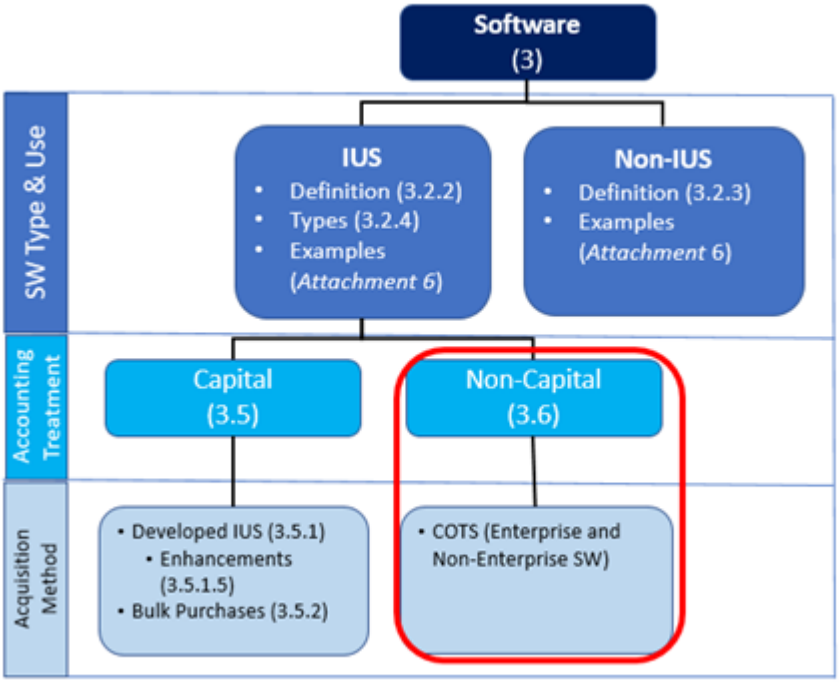
3.5.2.4.1.4. Disposal is not complete unless all copies of the decommissioned IUS are uninstalled from the network through uninstall procedures or proper disposition of the computer hardware or hard drive upon which the software is installed. Before uninstalling the software, BSLM will inform end users, including records managers, to save files created in the software, if necessary, to a commonly accessible (non-proprietary or open) file format and to save electronic records created in the software to a National Archives-approved file format with the original metadata if feasibly possible. (T-1):

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).

3.5.2.4.3. Per FAR 7.503(c)(11), ensure that disposal is performed by government personnel only, unless contractors are given specific authority to dispose of property at prices within specified ranges and subject to reasonable conditions as deemed appropriate by the AF. (T-1).

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 DAF 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 DAF 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 DAF software will be procured using applicable buying programs (in order of precedence):

3.6.3.1.1. DAF 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. 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 **Figure A7.2**, and **Figure A7.3**.

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.

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

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

3.6.4.1.7. 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 **Figure A7.4**.

3.6.6. **Disposal Process** .

3.6.6.1. The USLM will dispose of software in accordance with the terms of the license agreement. (T-1). Methods that may comply with license agreement terms include:

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. (T-1). Disposal is not complete unless these actions are taken.

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. (T-1). This will include a statement verifying that all media, licenses, and documentation have been destroyed or returned to the vendor.

3.6.6.5. Per FAR 7.503(c)(11), ensure that disposal is performed by government personnel only, unless contractors are given specific authority to dispose of property at prices within specified ranges and subject to reasonable conditions as deemed appropriate by the AF. (T-1).

Lauren BARRETT KNAUSENBERGER, SES
Chief Information Officer

(KIRTLANDAFB)

JASON F. VATTIONI, Colonel, USAF
Commander, 377th Air Base Wing

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 Subtitle I, Chapter 9, *Agency Chief Financial Officers*

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

Executive Order 13589, *Promoting Efficient Spending*

National Institute of Standards and Technology, SP 800-88 Rev. 1, *Guidelines for Media Sanitization*, December 2014

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

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

AFI 17-101, *Risk Management Framework (RMF) for Air Force Information Technology (IT)*, 6 February 2020

AFMAN 17-1303, *Air Force Cybersecurity Workforce Improvement Program*, 12 May 2020

DAFPD 17-2, *Cyber Warfare Operations*, 27 October 2020

AFPD 16-7, *Special Access Programs*, 21 November 2017

AFI 16-701, *Management, Administration and Oversight of Special Access Programs*, February 2014

AFPD 10-6, *Capability Requirements Development*, 6 November 2013

DAFI 90-160, *Publications and Forms Management*, 14 April 2022

DODI 5000.87_ DAFI 63-150, *Operation of the Software Acquisition Pathway*, 11 August 2021

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

DOD FMR 7000.14-R, Volume 1, Chapter 9, *Financial Records Retention*, February 2021

DOD FMR 7000.14-R, Volume 3, Chapter 8, *Standards for Recording and Reviewing Commitments and Obligations*, February 2020

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

DOD FMR, 7000.14-R, Volume 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*, January 2021

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

DODM 5200.01V3_AFMAN 16-1404V3, *Information Security Program: Protection of Classified Information,* 12 April 2022

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),* 2 March 2017

DODI 8320.04, *Item Unique Identification (IUID) Standards for Tangible Personal Property*, 3 September 2015

Federal Financial Accounting Technical Release (TR) 16, *Implementing Guidance for Internal Use Software*, 2016

Statement of Federal Financial Accounting Standard (SFFAS 10): *Accounting for Internal Use Software*, 9 October 1998

ODNI, *Improving Cybersecurity for the Intelligence Community Information Environment Implementation Plan* August 2019

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

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

DODI 5000.64_DAFI 23-111, *Accountability and Management of DoD Equipment and Other Accountable Property*, 6 December 2021

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, *Enterprise Risk Management and Managers' Internal Control Program Procedures,* 17 September 2020

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

AFMAN 16-1404 Volumes 1 *Information Security Program: Overview, Classification and Declassification*, 6 April 2022

AFMAN 16-1404 Volumes 2 *Information Security Program: Marking of Classified Information*, 7 January 2021

AFMAN 16-1404 Volumes 3 *Information Security Program: Protection of Classified Information*, 12 April 2022

AFMAN 63-144, *Business Capability Requirements, Compliance, and System Acquisition*, 25 July 2018

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

Prescribed Forms

(**Added-KIRTLANDAFB**) KIRTLANDAFB Form 3215, *Communications System Requirements Document (CSRD)*

(**Added-KIRTLANDAFB**) KIRTLANDAFB Form 578, *Information Technology (IT) Tracking Record*

AF Form 7500, Internal Use Software Cost Tracking

Adopted Forms

(**Added-KIRTLANDAFB**) AF Form 1297, *Temporary Issue Receipt*

DD Form 200, Financial Liability Investigation of Property Loss

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

DD Form 1150, *Request for Issue/Transfer/Turn-In*

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

(Added-KIRTLANDAFB) 377 ABW—377 Air Base Wing

(Added-KIRTLANDAFB) 377 MSG/SC—377 Mission Support Group/Communication Division

ACC—Air Combat Command

(Added-KIRTLANDAFB) ADPE—Automated Data Processing and Equipment

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFMC—Air Force Materiel Command

AFPD—Air Force Policy Directive

(Added-KIRTLANDAFB) AFRC—Air Force Reserve Command

(Added-KIRTLANDAFB) AFRIMS—Air Force Records Information Management System

AIT—Automated Identification Technology

(Added-KIRTLANDAFB) ANG—Air National Guard

APO—Accountable Property Officer

APR—Accountable Property Records

APSR—Accountable Property System of Record

ATP—Authority to Proceed

AUIC—Accountable Unit Identification Codes

(Added-KIRTLANDAFB) BECO—Base Equipment Control Officer

BSLM—Base Software License Manager

CAGE—Commercial and Government Entity code

CCC—Cyberspace Capabilities Center

CDRL—Contract Data Requirements List

(Added-KIRTLANDAFB) CFP—Communications Focal Point

CIP—Construction in Progress

CLIN—Contract Line-Item Number

CO—Contracting Officer

COCO—Contractor Owned/Contractor Operated

COGO—Contractor Owned/Government Operated

COTS—Commercial-Off-the-Shelf

(Added-KIRTLANDAFB) CSRD—Communications System Requirements Document

CST—Client Systems Technician

(Added-KIRTLANDAFB) CST—Client Support Technician

DAF—Department of the Air Force

DAFECO—Department of Air Force Equipment Control Office

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

DODI—Department of Defense Instruction

(Added-KIRTLANDAFB) DOE—Department of Energy

DPAS—Defense Property Accountability System

DPI—Digital Printing & Imaging

DRA—Defense Reporting Activity

DRMS—Defense Reutilization and Marketing Service

DRU—Direct Reporting Unit

EPL—Evaluated 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 Officer

FO—Functional Owner

FOA—Field Operating Agency

GE—General Equipment

GFP—Government Furnished Property

GOCO—Government Owned/Contractor Operated

GOGO—Government Owned/Government Operated

GPC—Government Purchase Card

GSA—General Services Administration

GSU—Geographically Separated Unit

HTSA—Host Tenant Support Agreement

IA—Information Assurance

(Added-KIRTLANDAFB) IAW—In Accordance With

IO—Information Owner

ISR—Intelligence, Surveillance, and Reconnaissance

ISSO—Information System Security Officer

IT—Information Technology

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 Agreement

(Added-KIRTLANDAFB) KAFB—Kirtland Air Force Base

KSD—Key Supporting Document

LDD—Limited Deployment Decision

MAJCOM—Major Command

MDA—Milestone Decision Authority

MFR—Memorandum for the Record

MOA—Memorandum of Agreement

MPS—Managed Print Services

(Added-KIRTLANDAFB) NAF—Non Appropriated Funds

OPR—Office of Primary Responsibility

PA—Property Administrator

PC—Property Custodian

PM—Program/Project Manager

PMO—Program Management Office

POC—Point of Contact

PSM—Product Support Manager

QRG—Quick Reference Guide

RFP—Request for Proposal

FLI—Financial Liability Investigation

SaaS—Software as a Service

SAE—Service Acquisition Executive

SAP—Special Access Program

SBA—Software Benefits Administrator

SCIF—Sensitive Compartmented Information Facility

SFFAS—Statement of Federal Financial Accounting Standards

SIM—Serialized Item Management

SKU—Stock Keeping Unit

SLIN—Sub-line numbering

(Added-KIRTLANDAFB) TCO—Telephone Control Officer

UAPO—Unit Accountable Property Officer

(Added-KIRTLANDAFB) UECO—Unit Equipment Control Officer

UIC—Unit Identification Code

USLM—Unit Software License Manager

(Added-KIRTLANDAFB) WCO—Wing Cybersecurity Office

Terms

(Added-KIRTLANDAFB) 377 MSG/SC—The Kirtland Air Force Base Communications Division. The Host Installation Accountable Property Officer.

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.

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.

(Added-KIRTLANDAFB) Accountable Unit Identification Code (UIC)—Previously called a Defense Reporting Activity (DRA) The AUIC is the master account assigned to KAFB for tracking and reporting accountability of all base ADPE assets. All UAPO accounts are created under AUIC FU4469

APSR—Is the property management system that used to control and manage accountable property records. Defense Property Accountability System (DPAS) – is a designated APSR for DAF.

(Added-KIRTLANDAFB) Automated Date Processing and Equipment (ADPE)—An information technology asset, or an organization which controls information technology assets.

(Added-KIRTLANDAFB) Base Enterprise Asset—Any device owned or managed by the 377 MSG/SC. Examples are but are not limited to, network switches, routers, servers, etc.

(Added-KIRTLANDAFB) Base Equipment Control Officer (BECO)—The individual appointed by the 377 MSG/SC as the primary point of contact for the retention, distribution, and disposition of all base accountable IT assets.

(Added-KIRTLANDAFB) Cannibalization—the removal of any internal system component, except for hard drives, (IE RAM, Video Cards, etc.), or any external power supply required for functional operation.

(Added-KIRTLANDAFB) Defense Logistics Agency (DLA)—The organization authorized by the government to receive excess equipment.

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.

(Added-KIRTLANDAFB) Government Furnished Equipment/Government Furnished Property (GFE/GFP)—Any accountable IT asset purchased by the government and given to a contractor. Any accountable IT asset purchased by a contractor with an expectation of government reimbursement. Any accountable IT asset purchased by the contractor and turned over to the government, either during the contract or at the end of a contract.

(Added-KIRTLANDAFB) Information Technology Asset User—A person who uses any information technology hardware, software, or telephonic device.

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.

(Added-KIRTLANDAFB) KIRTLANDAFB Form 3215, Communications System Requirements Document (CSRD)—The form used to request approval for all communication purchases, services, and connection authorizations.

(Added-KIRTLANDAFB) Like Item—Any IT asset that has an equal to or greater capability, then the initial asset identified.

(Added-KIRTLANDAFB) Personal IT Devices—Are Information Technology or Telephonic devices which include but are not limited to Cell phones, cell phone chargers, cameras, computers, laptops, tablets, hard drives, thumb drives, printers, thin clients, switches, routers, servers, VoIP phones, VTC equipment, or any custom-built IT or Telephonic devices, which belong to any individual, business, corporation, non-Air Force Agency, or foreign country.

(Added-KIRTLANDAFB) Property Custodian (PC)—An individual appointed by a unit APO to manage, inventory, receive and account for all unit-controlled IT assets.

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.

(Added-KIRTLANDAFB) Telephone Control Officer (TCO)—The individual appointed by a unit, as the primary point of contact for all unit telephone requirements.

(Added-KIRTLANDAFB) Tenant Accountable Property Officer (Tenant APO)—The commander of a tenant unit who does not have property account services provided by the Host APO.

(Added-KIRTLANDAFB) Unit Equipment Control Officer (UECO)—The individual appointed by the Host APO to directly manage UAPO specific property accounts. The primary point of contact for the management, retention, distribution, and disposition of all accountable IT assets within a specific unit's sphere of control.

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. The DPAS Site ID is FF-GEIT. Additional guidance will be provided by Air Force/A2/6 for SCI and national ISR assets.

A2.1.1. GOGO and GOCO APR and/or AR type IT assets will be accounted for in DPAS. (T-0).

A2.1.2. GOCO APR and/or AR type IT assets may be accounted for in an APSR other than DPAS with an approved waiver from SAF/CN. The alternative APSR must meet the requirements outlined in DODI 5000.64, section 4.3. waiver. (T-0).

A2.1.2.1. If an APSR waiver is approved by SAF/CN:

A2.1.2.1.1. Contractor must adhere to standards for asset accountability outlined in DODI 5000.64 and this manual (i.e., inventory, data attributes, etc.) and per contract obligations.

A2.1.2.1.2. To meet audit requirements, the contractor must provide asset reports containing required data elements per DODI 5000.64, section 4.6, within 3 business days of receiving the request. (T-0).

A2.1.3. COCO or COGO APR and/or AR type IT assets will be accounted for per contract obligations. (T-0).

A2.2. DPAS Roles and Responsibilities. Table A2.1 identifies DPAS roles and the corresponding Air Force personnel as prescribed in **paragraph 1.2**. **Table A2.2** identifies DPAS site structure and the corresponding Air Force structure.

Table A2.1. Air Force roles in DPAS.

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

Table A2.2. Air Force Structure in DPAS.

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 DAFECO is the IO for DPAS and must review/approve all access requests for Property Administrators and Auditors. (T-0). Requesting access to DPAS must be accomplished via the DAFECO SharePoint site. (T-1). 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. (T-0).

A2.2.1.2.1. Users requesting a new role be added or updated must submit a Role Request Form to the IO. (T-0).

A2.2.1.2.2. Users requesting a UIC be added or updated to their role must submit a Role Request Form and valid appointment letter to the IO. (T-0).

A2.2.1.2.3. Users requesting to be immediately removed from DPAS must submit a digitally signed email to the IO at **DAFECO.SAR.REQUESTS@us.af.mil**. (T-0).

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.

A2.2.1.4. Will review, validate, and process System Change Requests (SCR) for DPAS when issues are identified by the PA. (T-1).

A2.2.2. **Accountable Property Officer (APO).**

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

A2.2.3. **Property Administrator (PA): ECO or PC.**

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

A2.2.3.2. Receives and enters new asset records into DPAS via the Asset Receiving function.

A2.2.3.3. Processes receipt, transfer, and disposition of all accountable IT assets in DPAS.

A2.2.3.3.1. Ensures appropriate documentation is generated and attached to asset transfers from UIC to UIC and/or custodian to custodian (DD Forms 1149, 1150, 1348-1A, or locally generated transfer form). (T-1).

A2.2.3.3.2. Ensures assets on loan to a contractor be classified as GFP.

A2.2.3.3.2.1. 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.)

A2.2.3.3.3. Must designate and allocates excess assets. (T-1).

A2.2.3.4. Ensures an appropriate KSD is attached to every asset transaction using the attachment data field associated with the asset record in accordance with **Attachment 5**. (T-1).

A2.2.3.5. Ensures all accountable non-capital assets are entered into DPAS with the asset's fund code and capital code A. POC for fund codes will be the servicing resource advisor or contracting office. (T-1).

A2.2.3.5.1. Ensures all capital assets are loaded into the APSR in accordance with **paragraph 2.7.3** (T-1).

A2.2.3.6. Add or delete Unit Identification Codes (UIC) as necessary within their area of responsibility.

A2.2.3.7. Add, update, or delete custodian accounts as necessary within their area of responsibility.

A2.2.3.8. Request new catalog records to the DPAS Catalog Manager/DAFECO via the DAFECO ITAM DPAS SharePoint site.

A2.2.3.9. Will ensure all assets entered into DPAS have been coded only with one of the following condition codes. (T-0).

Table A2.3. Air Force Structure in DPAS.

Condition Code	Condition Code Definition
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 (spares are set at 5% of current inventory).
F	Use when the asset may still be utilized/is reparable.
G	Use when the asset is missing components.
H	Use when the asset is condemned or non-reparable
Note: Use "F, G, or H" when assets are ready for turn in to DLADS. Select based on asset condition (assets must be out of warranty to be turned into 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 accountable assets have DPAS-generated bar code labels containing serial number and item description affixed. (T-1).

A2.2.5. **Data Inquiry.**

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

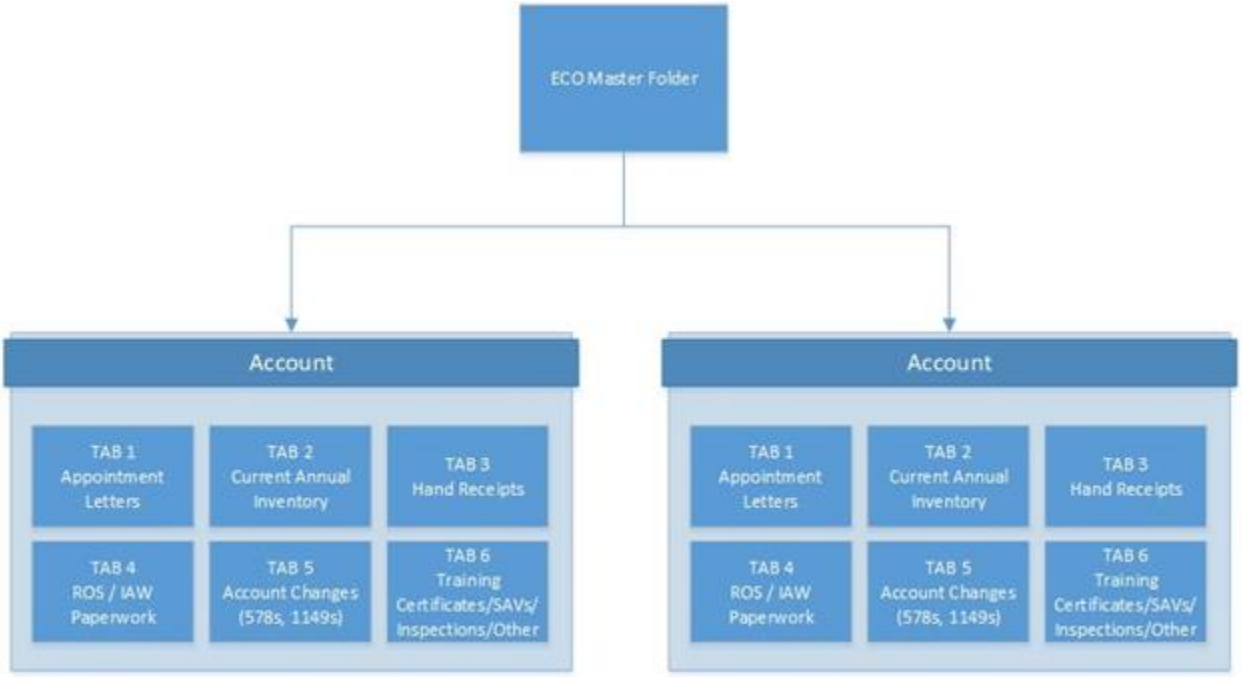
A2.2.6. **Forms and Reports.**

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

Attachment 2 (KIRTLANDAFB)

ACCOUNT RECORD STRUCTURE

Figure A2.1. (KIRTLANDAFB) Account Record Structure.



Attachment 3

TECH REFRESH GUIDANCE FOR STANDARD LAPTOP AND DESKTOP COMPUTERS.

A3.1. Purpose and Scope.

A3.1.1. Purchases of standard laptop or desktop computers outside this tech refresh guidance will require either an approved/completed AIS work order (i.e. CIPS/REMEDY) or a locally generated document containing the UAPO's justification and approval for purchase. (T-0).

A3.1.2. Assets eligible for refresh will be any assets exceeding the refresh cycle identified in **Table A3.1** according to the manufacturer year loaded in DPAS. Assets identified to be refreshed will not exceed 25% of total inventory for each individual AUIC in any given year.

Table A3.1. Standard Laptop and Desktop Computer Refresh Rate.

Device Type	Refresh Lifecycle	Refresh Rate per year
Desktop	4 years	No more than 25%
Laptop/Notebooks	4 years	No more than 25%

A3.1.3. Each May, DAFECO office will provide a listing of assets that are eligible for refresh in the next fiscal year to each MAJCOM/ FLDCOM A6, DRU. (T-1). The asset listings will be posted on the SharePoint site: **https://usaf.dps.mil/teams/ccc/itam/SitePages/Home.aspx**.

A3.1.4. The final determination of how many assets will be refreshed will be determined by the MAJCOM/ FLDCOM A6, DRU, or FOA based on their review of the asset refresh listings provided by the DAFECO and cost projections submitted for POM. (T-1). Final decisions on quantity and funding will be disseminated by the MAJCOM/ FLDCOM A6, DRU or FOA. (T-1).

A3.1.5. Funding dependent, the target for annual tech refresh will be up to 25% of eligible laptops and/or desktops per year, with the goal of 100% tech refresh occurring every 4 years. (T-1). If the computers eligible for tech refresh exceed 25% of inventory, MAJCOM/ FLDCOM A6, DRU, or FOA may request a waiver from SAF/CN for additional purchases to refresh those assets. (T-0).

A3.1.6. When reviewing assets for tech refresh, MAJCOM/ FLDCOM A6, DRU, or FOA should strive to achieve the most mobile solution. (T-1). Any desktop that can be replaced by a laptop will enhance the enterprise's mobile posture and contingency operations.

A3.1.7. Any computer purchases as part of a tech refresh will meet ITCC's current technical requirements and will be procured per **paragraph 2.5** (T-0).

A3.1.8. Assets must be delivered directly to the base warehouse per established procedures for each location. (T-1).

A3.2. Roles and Responsibilities for Tech Refresh.

A3.2.1. **Air Force Equipment Control Office (DAFECO).**

A3.2.1.1. Every May, DAFECO will identify tech refresh eligible assets for the next fiscal year utilizing DPAS and AFMAN 17-1203, Table A3.1. (T-1).

A3.2.1.2. Asset refresh listings created by DAFECO will include the following data: AUIC, UIC, Custodian Account, and estimated refresh costs. (T-1). The list will be posted to the DAFECO SharePoint site for each MAJCOM/ FLDCOM A6, DRU, or FOA. The following data attributes will be included on the tech refresh listings:

Table A3.2.

Data Attributes
Actbl_UIC
UIC
Custodian Nbr
MajorCommand (or Major Cmd Cd)
Stock_Nbr
Item_Desc
Location
Sub_Loc
Mfr_Name
Mfr_Yr
Mfr_Model_Nbr
Mfr Part Nbr
Serial_Number
Fund_Cd
Total_Cost
Acq_Date

A3.2.2. **MAJCOM/FLDCOM A6, DRU, FOA**

A3.2.2.1. MAJCOM/ FLDCOM A6, DRU, or FOA will review the asset tech refresh listing annually for tech refresh requirements and justification for funding. (T-1).

A3.2.2.2. MAJCOM/ FLDCOM A6, DRU, or FOA will plan for and disseminate approval of funding and purchasing data requirements to their units. (T-1).

A3.2.3. **Equipment Control Officer (ECO).**

A3.2.3.1. ECOs will accept deliveries and load assets into DPAS within 7 calendar days of receipt. (T-1).

A3.2.3.2. ECOs will distribute assets to unit PCs in accordance with AUIC/UIC/Account requirements. (T-1).

A3.2.3.3. ECOs will work with PCs to complete one for one asset swaps within 30 calendar days (90 calendar days for ANG) of receiving replacement assets. Assets being replaced will be condition coded "F, G, or H" in DPAS, depending on asset's status, and then turned in to DLADS. (T-1).

A3.2.4. **Property Custodian (PC).**

A3.2.4.1. PCs will work with the ECOs to complete one for one asset swaps within 30 calendar days (90 calendar days for ANG) of receiving replacement assets. (T-1).

A3.2.4.2. PCs will work with the ECOs to coordinate deployment of new assets.

A3.2.4.3. PCs will replace old assets with new assets within 30 days and notify ECOs when exchange is complete.

A3.2.4.4. PCs will dispose of assets to DLADS within 60 days of exchange and provide ECOs with DLADS documentation showing completion of asset disposal.

Attachment 4

IT HARDWARE ENTERPRISE INVENTORY PLAN.

A4.1. Purpose and Scope.

A4.1.1. 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/FLDCOM/DRU/FOA organization will be articulated in a MAJCOM/FLDCOM/DRU/FOA-specific Inventory Plan. (T-1). Additional guidance may be provided by Air Force/A2/6 for SCI and national ISR assets.

A4.2. Inventory Frequency.

A4.2.1. All Hardware Assets meeting the criteria stated in **paragraph 2.4.3** and **paragraph 2.4.4** are accountable and will be inventoried annually. (T-0).

A4.3. Preparing for Inventory.

A4.3.1. 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).

A4.3.1.1. 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).

A4.3.2. To assist in this process, the account owner can use a combination of asset discovery/automated inventory tools and manual identification of assets.

A4.3.2.1. 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.

A4.3.3. This discovery cannot be done any earlier than one month prior to the inventory due date. (T-1).

A4.3.4. 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.

A4.4. Performing the Inventory.

A4.4.1. To perform an asset inventory, the PC will:

A4.4.2. Ensure that all assets in their account(s) have been identified. (T-1).

A4.4.3. Ensure that gains/losses against the inventory baseline are documented and reconciled. (T-1).

A4.4.4. If using Automated Inventory Tool (AIT), the physical inventory will be performed only on those assets not identified using the AIT. (T-1).

A4.4.5. To inventory remote or teleworking assets, the PC will review documentation (AF Form 1297 Hand Receipt or locally established documentation) for assets assigned to remote workers and then contact the assigned individual to ensure the asset remains in their possession. (T-1). The individual assigned the asset(s) being inventoried will respond to the PC with a digitally signed email or digitally signed memorandum certifying they still possess the asset(s). (T-1).

A4.5. Completing the Inventory. To complete an asset inventory, the UAPO will:

A4.5.1. Ensure that the individual performing the inventory has signed, indicating that the inventory is complete and accurate. (T-1).

A4.5.2. Endorse the signed inventory with signature, accepting responsibility for the results. (T-1).

A4.5.3. Will provide the completed, signed, and endorsed inventory in an electronic format to the installation ECO for record. (T-1).

A4.5.4. Upon signature, PA will store signed documentation in file plan and update the date of last inventory for all assets within the account in the APSR. (T-1).

A4.6. Finalizing the Inventory. To finalize an asset inventory, the ECO will reconcile all gain/loss annotations in DPAS. (T-1).

A4.7. Random Sampling. DAFECO will perform random sampling of IT asset enterprise to ensure inventory requirements are being adhered to. (T-1).

Attachment 5

IT HARDWARE KEY SUPPORTING DOCUMENTS (KSDS) AND MANDATORY DATA ELEMENTS.

A5.1. 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/FLDCOM/DRU/FOA organization will be articulated in a MAJCOM/FLDCOM/DRU/FOA-specific plan. (T-1).

A5.2. IT Asset Life Cycle. KSDs will be retained throughout the following phases of the asset life cycle:

A5.2.1. Plan. This phase includes activities in which the asset requirement is generated and approved. (T-1).

A5.2.2. 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).

A5.2.3. Fielding. This phase includes activities in which the asset arrives at the warehouse, entered into the DPAS, staged for fielding, and fielded. (T-1).

A5.2.4. Management. This phase includes activities in which the asset is inventoried, transferred, and updated. (T-1).

A5.2.5. Retirement. This phase includes activities in which asset disposition is requested, staged for disposition, sent to DRMS/DLADS, and updated in DPAS. (T-1).

A5.3. Retaining KSDs.

A5.3.1. 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).

A5.3.1.1. DPAS will serve as the primary records management system, but UAPOs and ECOs may determine and follow additional local procedures. (T-1).

A5.3.1.2. Below table outlines requirements for which transactions must include a KSD, minimum data requirements for each KSD, and responsible parties. (T-1).

Table A5.1. Key Supporting Documents (KSDs) Requirements.

Life Cycle Transaction	Key Supporting Document (KSD)	Retention	Mandatory Data Elements	Acceptable Range of Documents	Responsible Entity
Requirement generated	IAW local process	IAW Local File Plan	IAW local process	IAW local process	PC
Requirement approved	IAW local process	IAW Local File Plan	IAW local Process	IAW local process	PC
Order generated	Web based activity	IAW Local File Plan	IAW local process	IAW local process	PC
Order approved	Web based activity	IAW Local File Plan	IAW local process	IAW local process	PC and ECO
Funds executed, shipped to customer	Web based activity	IAW Local File Plan	IAW local process	IAW 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	DPAS transaction /document	PC
Transfer	DPAS transaction	Mandatory	Old location, new location	DPAS transaction, DD Form 1149, 1150 or locally generated transfer form	PC and ECO
Location updated	DPAS transaction/document	Mandatory	Old location, new location	DPAS transaction /document	PC and ECO
Disposition requested	DPAS transaction	Mandatory	Date, price, serial, part, manufacturer CAGE	DPAS transaction	PC and ECO
Serviceable asset advertised	Web based activity	Conditional	Conditional	Conditional	ECO
Staged for disposition	DPAS transaction/document	Mandatory	Date, price, serial, part, manufacturer CAGE	DPAS transaction	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, manufacturer CAGE	DD Form 1348-1A, ETIDs, MFR	PC and ECO

Attachment 6

IUS AND NON-IUS EXAMPLES.

Table A6.1. 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,	YES		Defense Enterprise Accounting and

Definition	IUS		Examples
human resources, supply chain, and customer information) that are integrated within the core system or interfaced to external systems.			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
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			

Definition	IUS		Examples
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)			

Definition	IUS		Examples
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
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 7

PROCESS FLOW CHARTS.

Figure A7.1. Developed IUS Acquisition, Development and Deployment Process.

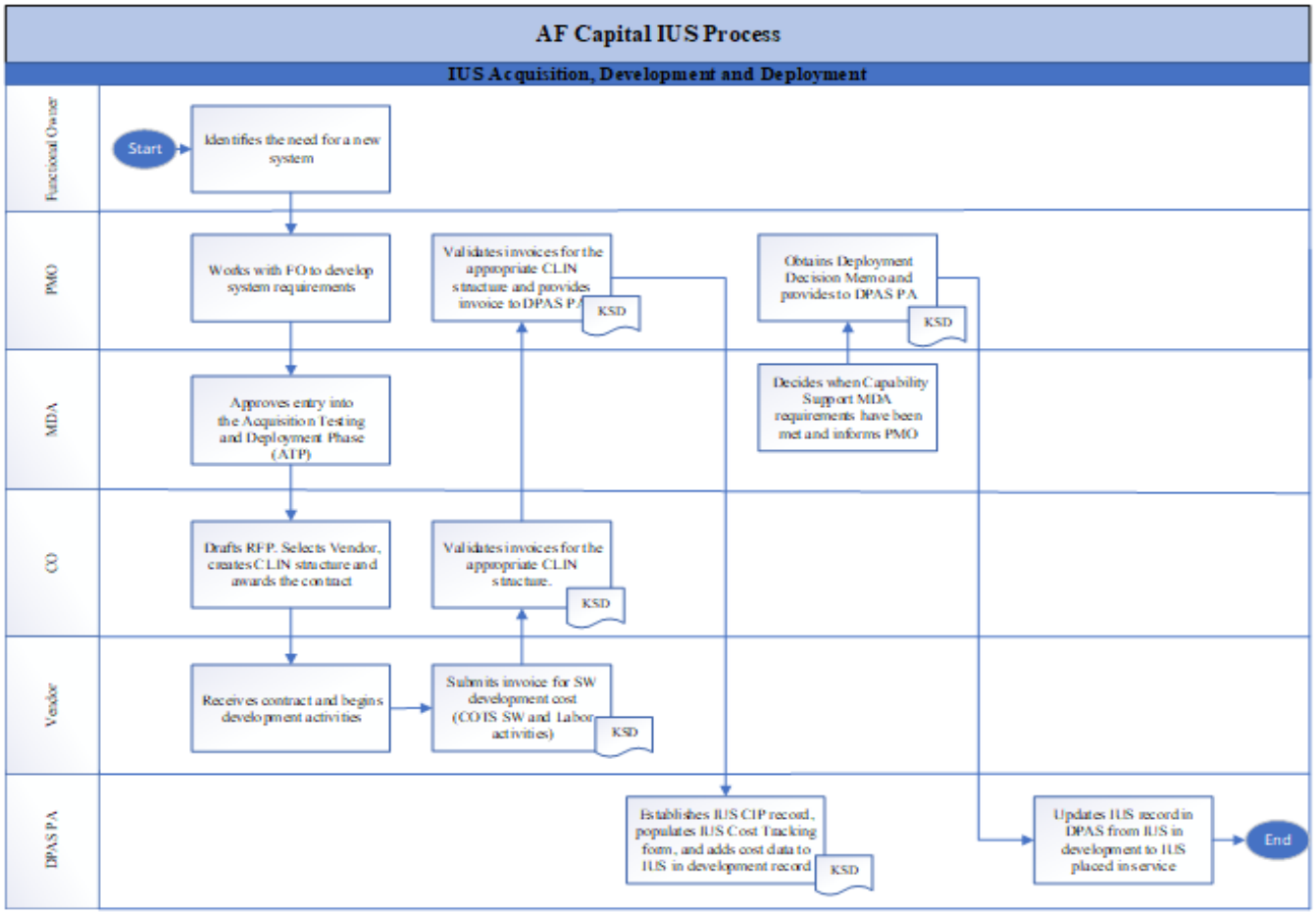


Figure A7.2. Enterprise Software Acquisition and Deployment Process.

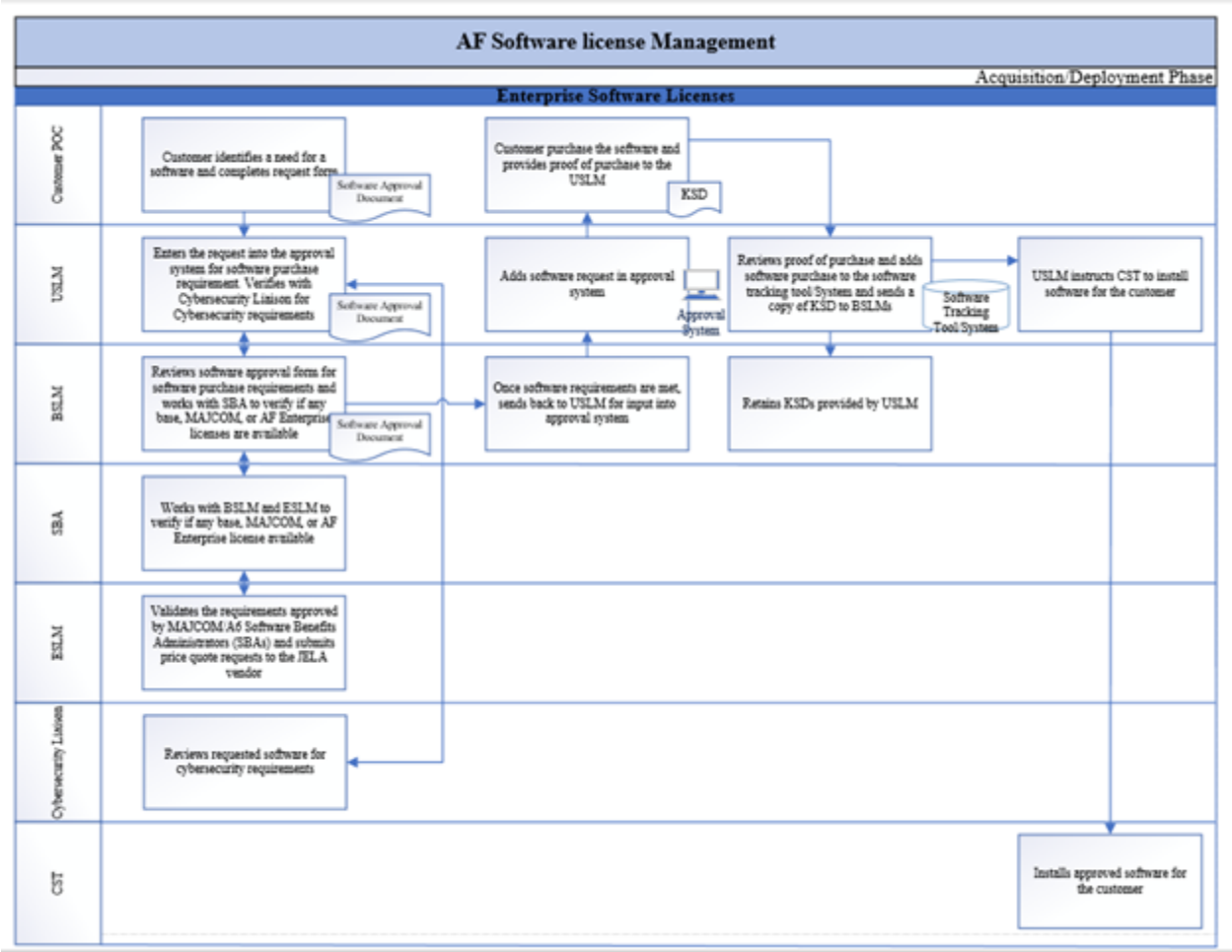


Figure A7.3. Non-Enterprise Software Acquisition and Deployment Process.

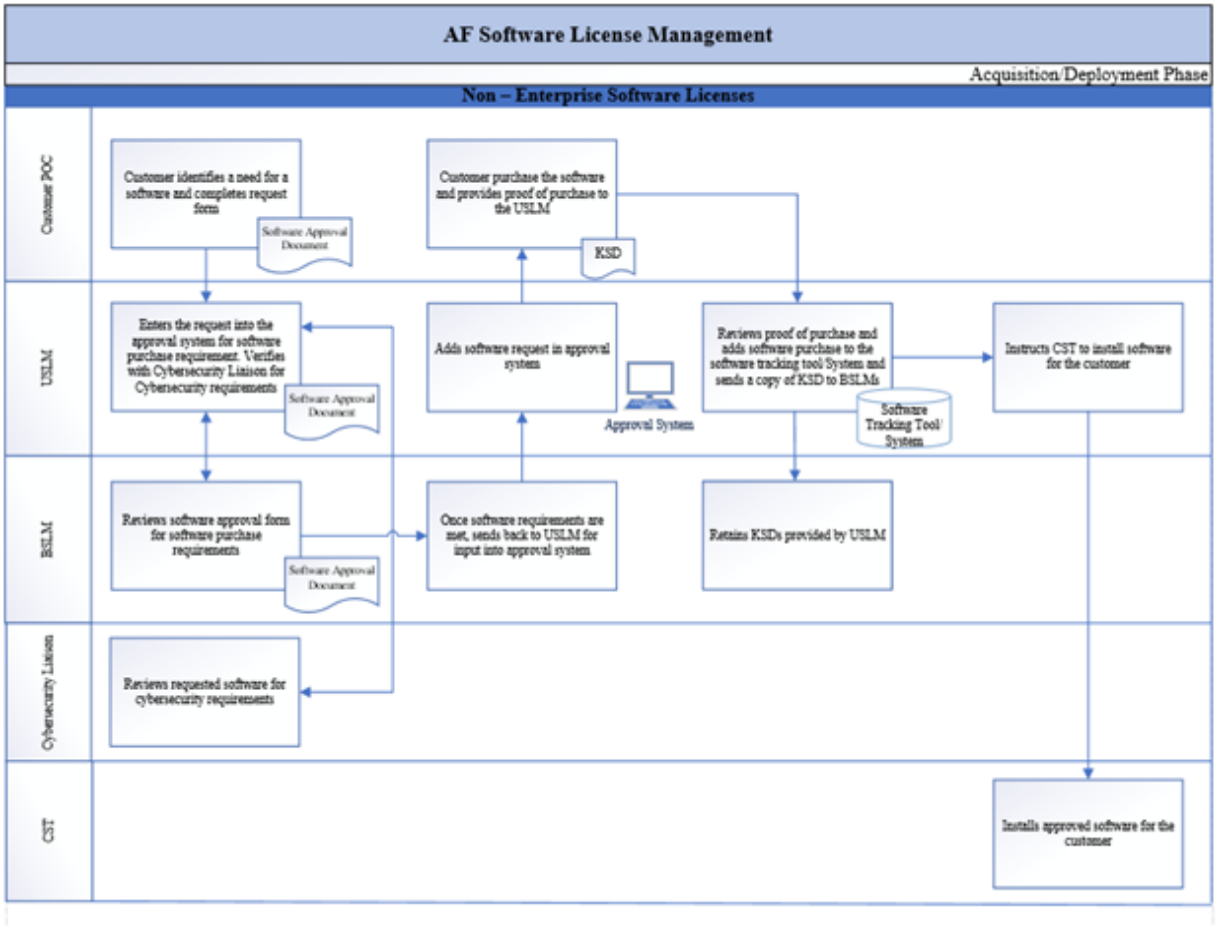


Figure A7.4. Software Annual Inventory Process.