MEMORANDUM FOR ALL MAJCOM-FOA-DRU-CV-DISTRIBUTION C

FROM: SAF/D-CIO

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

By Order of the Secretary of the Air Force, this Air Force Guidance Memorandum immediately changes AFMAN 17-1203, Information Technology (IT) Asset Management (ITAM) 18 May 2018. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications, the information herein prevails, IAW AFI 33-360, Publications and Forms Management, 1 Dec 2016.

This AFGM incorporates Attachment 4, Standard Operating Procedure (SOP) for Internal Use Software (IUS) Accountability into Chapter 3, Software Asset Management of AFMAN 17-1203, 18 May 2018. This SOP addresses required financial accountability of IUS as outlined in applicable Department of Defense (DoD) and Financial Management Regulation (FMR) directives and applies to all Air Force activities and Air National Guard and US Air Force Reserve units.

Additionally, in alignment with HAF/A4, SAF/D-CIO has begun planning and migration activities to meet a 31 March 2019 transition from AF Equipment Management System – Asset Inventory Management (AFEMS-AIM) to the Defense Property Accountability System (DPAS). In support of this migration, 38 CYRS/AFECO team will be reviewing and revising policy and processes, establishing training guides, and providing updates on our status and progress.

This memorandum supersedes the previous version and becomes void after one year has elapsed from the date of this memorandum, upon incorporation by interim change to, or rewrite of Air Force Manual 17-1203, whichever is earlier.

WILLIAM E. MARION II, SES, DAF
Deputy Chief Information Officer

Attachment:
Attachment 4
Standard Operating Procedure (SOP) For Internal Use Software (IUS) Accountability

Procedure Owner: SAF/CIO A6

Date: 19 Oct 2018

Version: 1.00
1. OVERVIEW. This Standard Operating Procedure (SOP) provides definitions, terms, processes, and procedures for properly accounting for IUS throughout the AF. The initial focus of this guidance is on contractor-developed software. An updated version of this document will provide further guidance on Commercial-Off-The-Shelf (COTS) and internally developed software. Appendix D: GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION, provides a list of all applicable references and guidance pertaining to the accountability of IUS. The requirement for IUS accountability and auditability is identified in the National Defense Authorization Act for Fiscal Year 2010 (FY10 NDAA), Section 1003, Audit Readiness of financial statements of the Department of Defense establishes the requirement for IUS accountability and auditability through the development of the Financial Improvement and Audit Readiness (FIAR) Plan and has been declared an Assessable Unit (AU) under General Plant, Property & Equipment (PP&E).

For all inquiries and further guidance, contact the Secretary of the AF, Chief, Information Dominance & Chief Information Officer (SAF/CIO) A6SE IT Asset Management (ITAM) Office at: usaf.pentagon.rsrcmgmt.mbx.saf-cio-a6-itam-workflow@mail.mil.

2. BACKGROUND. IUS that meets the criteria for capitalization, in accordance with Generally Accepted Accounting Principles (GAAP), must be reported on DoD financial statements within the General Property, Plant, and Equipment (PP&E), Net Line on the Balance Sheet, and as IUS within Note 9 of the financial statements.

2.1. An item is capitalized when it is recorded as an asset, rather than an expense. This means that the expenditure will appear on the balance sheet, rather than the income statement. One would normally capitalize an expenditure when it meets both of these criteria:

2.1.1. Development cost of the IUS asset over the project development cycle exceeds the capitalization limit of $250,000 (see Table 6.1 for costs eligible for capitalization). Expenditures below this threshold are deemed too immaterial to capitalize.

2.1.2. When completed, the finished asset will have a useful life of 2 years and more. If an expenditure produces value over a long period of time, then it should be recorded as an asset and, in the case of IUS, amortized over its useful life of 2-5, or 10 years.

2.2. The April 2015 Financial Improvement and Audit Readiness Guidance establishes IUS as a Mission Critical Asset category, as it is likely to be material to the financial statements of many Components (Military Services and Defense Agencies), and the DoD Consolidated Financial Statements.

2.3. Paragraph 3.8 of DoD Instruction (DoDI) 5000.76, Accountability and Management of Internal Use Software, March 2, 2017, requires that IUS assets be accounted for in an Accountable Property System of Record (APSR). In April 2018, HAF/A4 designated the DPAS application as the APSR.

3. PURPOSE AND SCOPE. This guidance provides processes to properly identify, account for, and financially report contractor-developed IUS that meets capitalization criteria. IUS that does not meet the capitalization threshold will not be governed by this process guide; additional guidance addressing the accountability of non-capital IUS will be forthcoming.
3.1. This guidance establishes procedures to comply with DoDI 5000.76, *Accountability and Management of Internal Use Software*, which relate to the lifecycle accountability and management of IUS, to include documenting IUS lifecycle events and transactions.

3.2. This SOP also follows the software development life cycle (SDLC) as outlined in DoDI 5000.02, *Operation of the Defense Acquisition System*, and DoDI 5000.76, *Accountability and Management of Internal Use Software*, and their supporting guidance.

3.3. Assigns responsibilities and provides procedures for maintaining property management and accountability of AF-owned IUS.

3.4. Defines the roles and responsibilities of AF IUS property managers and other officials with regard to IUS property management and accountability.


**Note 9. General PP&E, Net**

<table>
<thead>
<tr>
<th>As of September 30</th>
<th>2018 (unaudited)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Amounts in thousands)</td>
<td></td>
</tr>
<tr>
<td><strong>1. Major Asset Classes</strong></td>
<td><strong>2018</strong></td>
</tr>
<tr>
<td><strong>Buildings, Structures, and Improved Leasehold</strong></td>
<td>S/L</td>
</tr>
<tr>
<td><strong>Improvements</strong></td>
<td>S/L</td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td>S/L</td>
</tr>
<tr>
<td><strong>General Aircraft</strong></td>
<td>S/L</td>
</tr>
<tr>
<td><strong>Satellites</strong></td>
<td>S/L</td>
</tr>
<tr>
<td><strong>Other</strong></td>
<td>S/L</td>
</tr>
<tr>
<td><strong>Construction-in-Progress</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Military Equipment</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Real Property</strong></td>
<td>S/L</td>
</tr>
<tr>
<td><strong>Total General PP&amp;E</strong></td>
<td>S/L</td>
</tr>
</tbody>
</table>

4. **DEFINITION OF INTERNAL USE SOFTWARE.**

In general, "Software" includes the application and operating system programs, procedures, rules, and any associated documentation pertaining to the operation of a computer system or program. Most often, software is an integral part of an overall system(s) which is defined to include elements such as ...
hardware, infrastructure, personnel, training, documentation, procedures, controls, and data as well as their relationships.

4.1. IUS is:

4.1.1. Acquired or developed to meet the entity's internal or operational needs (intended purpose).

4.1.2. 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 the entity's internal or operational needs (software type).

4.1.3. IUS can be purchased from commercial vendors and is considered “commercial off-the-shelf (COTS), government of the shelf (GOTS), “modified "off-the-shelf", internally developed, or contractor developed. IUS includes software that is:

   4.1.3.1. Used to operate an entity's programs (e.g., financial and administrative software, including that used for project management).

   4.1.3.2. Used to produce the entity's goods and to provide services (e.g., maintenance work order management and loan servicing).

   4.1.3.3. Developed or obtained for internal use and subsequently provided to other federal entities with or without reimbursement.

4.1.4. To further determine whether an IT investment is IUS, refer to Appendix A: IUS ASSET DETERMINATION.

4.2. IUS is not:

4.2.1. Software embedded in equipment (to include weapons system and Special Test equipment). To further clarify, software embedded within an equipment asset is not solely excluded upon classification as such. The software must be necessary to operate the equipment, as intended, for the software to not be considered IUS. If the piece of equipment will operate as intended, upon removal of the software, the software shall be considered IUS. If the piece of 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 piece of equipment.

4.2.2. Computer software that is fully integrated and embedded into and necessary to operate general Property, Plant and Equipment (PP&E), rather than performing an application. This software shall be considered part of the PP&E, of which it is an integral part; therefore, capitalized and depreciated accordingly (e.g., airport radar, router, switches and computer operated lathes).

4.3. Types of IUS.

4.3.1. COTS Software.

   4.3.1.1. COTS software is acquired from a vendor “as-is” and configured to be ready for use with no to minimal modifications. COTS software seldom works alone. Development of reports, interfaces, conversions, and extensions (RICE) - such as interfaces to other systems,
may be a significant cost factor that enables the IUS to function. Such costs should be considered as part of a project cost in determining whether IUS is COTS or Developed IUS.

4.3.2. Developed Software.

4.3.2.1. Developed IUS can be developed by contractors or organic governmental personnel.

4.3.2.2. Most of the AF’s developed software meets or exceeds the $250K per project capitalization threshold over the project development cycle, as well as the 2 year useful life threshold, deeming it “capitalized IUS”.

4.3.2.3. Developed IUS assets that meets capitalization criteria are reported as assets on the financial statements in Note 9.

4.3.2.4. Where Developed IUS is reported differs during the time the asset is in development and when development is complete with the creation of a new IUS asset.

4.3.2.5. During development, capitalized costs are reported in IUS in development account. This account is used to record full cost amount incurred for those costs that are capitalized in accordance with Table 27-1 of DoD FMR Volume 4, chapter 27.

4.3.2.6. At the end of development and after acceptance as a completed IUS asset, the total accumulated development cost is established as the acquisition cost of the new IUS asset and reported as Software under section D of Note 10 of the financial statement.

4.3.3. Cloud Computing.

4.3.3.1. The FASAB defines a cloud computing service as “any resource that is provided over the internet and has the following characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.”

4.3.3.2. An entity that has the contractual right to the IUS licenses in a cloud environment is obligated to account for those licenses when they meet capitalization criteria.

4.3.3.3. The individual program’s cost of shared cloud services as well as those used exclusively for development of the IUS should be capitalized in the IUS in Development account and ultimately included as part of the cost of the IUS Software asset.

4.3.4. Shared Services.

Shared Services are defined as a “mission or support function provided by one business unit to one or more other business units within or between organizations”. In such cases, the funding and the resourcing is shared with the entity providing the shared service acting as the service provider. The federal government identifies three types of shared service structures:

4.3.4.1. Intra-Agency Shared Services. Intra-Agency includes services provided within the federal agency, without the boundaries of an organization, i.e. DoD. Commands that fund the COTS IUS licenses and related development will be responsible for accounting of the IUS.
4.3.4.2. **Inter-Agency Shared Services.** Interagency includes services provided by one federal agency to other federal agencies. Agencies or components that fund applicable COTS IUS licenses and related development will be responsible for accounting of the IUS.

4.3.4.3. **Commercial Shared Services.** Commercial Shared Services are services provided by commercial vendors. If the cost of licenses and development is funded by the commercial service provider, shared services shall not be accounted by the AF.

5. **ROLES AND RESPONSIBILITIES.**

5.1. **IUS Information Owner (IO).**

5.1.1. Serves as the AF level site owner for DPAS IUS.

5.1.2. Must be a government civilian or military member. Currently assigned to SAF/CIO A6.

5.1.3. Approves or disapproves DPAS organization accounts.

5.1.4. Provides APSR support to customers.

5.1.5. Annually validates the DoD Component APSR by utilizing DD Form 3041, APSR Requirements Checklist for IUS.

5.1.6. In coordination with APO and Program Managers (PM), ensures accountable records have the associated auditable information available for examination.

5.1.7. May delegate duties to additional IOs.

5.2. **Accountable Property Officer (APO).**

5.2.1. This is a Major Command (MAJCOM), Direct Reporting Unit (DRU), or 2-letter role.

5.2.2. Serves as the MAJCOM, DRU, or 2-letter level property officer for all capitalizable IUS assets owned by the organization, or where IUS that supports enterprise business activities do not fall cleanly under a parent major command, systems are managed under a portfolio (such as Logistics, Personnel, or Civil Engineering).

5.2.3. Ensures accountable records for their applicable organizations have the associated auditable information available for examination.

5.2.4. Ensures organization’s IUS is accounted for and reported by designated PMO in accordance with DoD management policies.

5.2.5. May delegate duties to additional APO to enable execution but the ultimate responsibility for execution remains with the APO.

5.2.6. Must be a government civilian or military member.

5.3. **Program Manager (PM).**

5.3.1. Role is designated in coordination with IUS owning organization’s APO from the Program Management Office (PMO) that develops, deploys, and sustains the IUS throughout its life-cycle.
5.3.2. Works with Contracting Officer (CO) and the AF IUS owner organization to draft Request for Proposal (RFP), in whole or in part, contains development of software purposed for internal use.

5.3.3. Supports the MDA in arriving at a determination of whether a developed IUS has reached Acquisition's Authority to Proceed (ATP) - Acquisition, indicating permission to incur project expenses in conformity with the Acquisition's Strategy. DoDI 5000.75, Business Systems Requirements and Acquisition, paragraph 1.2.e, establishes requirements applicable to ATPs which are “milestone-like events”. The MDA approves critical acquisition decisions for ATP decision points or concurs in contractual commitments.

5.3.4. Is responsible for IUS reporting through DPAS.

5.3.5. Collects and maintains all IUS Key Supporting Documents (KSD) in support of IUS as Software and IUS in Development.

5.3.6. Enters valid developed IUS cost data and uploads supporting KSD into IUS in Development records established in the APSR.

5.3.7. Updates status of IUS in Development to record that the IUS development for Projects or sub-Project is complete and uploads the Capability Production document, representing attainment of Capability Support ATP to the APSR.

5.3.8. Updates status of IUS in Development record in APSR to record that the IUS development for this Project or sub-Project is complete upon receipt of a MDA Acquisition Decision Memo (ADM) declaring achievement of ATP - Capability Support.

5.3.9. In coordination with the Program Sponsor/Owner, ensures CLIN structure identifies development activities that require capitalization, as detailed in Table 6.1.

5.4. Contracting Officer (CO).

5.4.1. Works with the PM to draft a RFP containing a statement of work and/or other form of requirement document(s) for IUS development.

5.4.2. Drafts RFPs and ultimately award contracts with statements of work that, in whole or in part, contain development and/or acquisition of software purposed for internal use.

5.4.3. Reviews the requiring activity document(s) that established separately identifiable line items for IUS on a purchase request and/or funding document.

5.4.4. Serves as contract advisor to requiring activities to provide contracting guidance in the Federal Acquisition Regulation (FAR), Part 7 - Acquisition Planning, Defense Federal Acquisition Regulation Supplement (DFARS), Part 207 - Acquisition Plans, and AF Federal Acquisition Regulation Supplement (AFFARS), Part 5307 - Acquisition Planning, where applicable.

5.4.5. Ensure that solicitation instructions, provisions, contract clauses and Contract Data Requirements Lists (CDRL) provided by the requiring activity are included in solicitations and contract awards as applicable.
5.4.6. Writes contract, in conjunction with the PM, per requirements detailed in Table 6.1 to itemize expenses requiring capitalization. Ensures CLIN and SLIN structure aligns with the lines of accounting assigned by requiring activities.

5.5. Contracting Officer Representative (COR).

Validates invoices for services performed that include developed IUS, for inclusion of valid Contract Line Item Number (CLIN) or CDRL content, and notifies the vendor when CLIN or CDRL content is invalid or missing.

5.6. Program Sponsor/Owner.

5.6.1. Program Sponsors/Owners requiring Developed IUS will work with PMs and Contracting Officer (CO) to ensure that there has been discussion and discovery of the types and appropriate quantities of IUS, based on bona fide need. Quantities of IUS being requested in acquisition plans, strategies, and execution, must be such that the CO is able to build the request into the contract provisions and address the special requirements of identifying IUS and Developed IUS.

5.6.2. Determines requirements are valid, capability requirements are achievable, and capability development efforts have feasible implementation plans.

5.6.3. Identifies and establishes that IUS is broken out on separately identifiable line items on purchase request/funding documents for the CO.

5.6.4. Can be APO, PM or proponent for IUS to be developed.

5.6.5. In coordination with the PM, ensures CLIN structure identifies development activities that require capitalization, as detailed in Table 6.1.

5.7. Asset Custodian (AC).

5.7.1. This role can be performed by the PM, Deputy PM, Product Support Manager (PSM) or any person designated by the PM.

5.7.2. Provides asset accountability support to Asset Managers at the program level.

5.7.3. Ensures all capitalized IUS is entered in the APSR.

5.7.4. Ensures all KSD are properly maintained and provided to appropriate personnel within DPAS.

5.7.5. Is accountable for all assigned IUS assets.

5.7.6. Is responsible for assets assigned to them. The Asset Custodian (AC) is designated by the APO. Each Unit Identification Code (UIC) in DPAS may have multiple ACs assigned.

5.7.7. Performs, at a minimum, an annual inventory of all assigned IUS assets recorded in DPAS.

5.7.8. Notifies PM of all IUS changes, moves, deletes, etc. that effect DPAS and provides the supporting KSD(s).

5.7.9. Notifies the PM of any lost or unaccounted for IUS.

5.7.10. Can be a contractor, government civilian or military member.
5.8. **Milestone Decision Authority (MDA).**

5.8.1. DoDI 5000.75, *Business Systems Requirements and Acquisition*, paragraph 1.2.e, establishes statutory requirements applicable to ATP which are “milestone-like events”. The MDA approves critical acquisition decisions for ATP decision points where, as described in paragraph 4.1.b., decisions will be informed by measures that assess the readiness to proceed to the next phase of the process. The MDA approves entry into the Acquisition Testing and Deployment Phase at ATP 3. ATP 3 is issued by the Acquiring organization indicating approval to incur project expenses in conformity with the Acquisitions Strategy and the terms of the contract.

5.8.2. At the Acquisition ATP checkpoint or milestone decision point, the MDA authorizes acquisition of the business system and approves continued execution of the updated implementation plan.

5.8.3. Determines when and whether Capability Support ATP, designating the completion of the IUS Development Process has been reached and documents that in an ADM.

5.8.4. Issues an ADM to the PMO once Capability Support ATP is determined to have been achieved. The ADM may serve as the evidence for:

   a) Discontinuance of further capitalization of development costs in IUS in Development record.

   b) Inactivation of reporting of IUS in Development balance.

   c) Creation of a new IUS asset in the APSR.

6. **ACCOUNTABILITY RULES.**

6.1. **General Accountability Rules.**

6.1.1. **Scope of Accountability.**

   The scope of accountability prescribed in this guidance is for all Developed IUS assets that meet or exceed the capitalization criteria of $250K per project over the project development cycle and that have a useful life of two or more years.

6.1.2. **IUS accountability will be established and maintained:**

   6.1.2.1. At the end of the development phase for government- or contractor-developed IUS. The end of the development phase for major automated information systems will be the Full Deployment Decision (FDD), as described in DoDI 5000.02, *Operation of the Defense Acquisition System*.

   6.1.2.2. Upon government acceptance of COTS IUS.

   6.1.2.3. Upon the completed transfer to another entity in the DoD Component inventory.

   6.1.2.4. By the acquiring organization in accordance with Department of Defense Financial Management Regulation (DoDFMR) 7000.14-R. If the acquiring organization does not have exclusive control over the IUS, the DoD Component that controls the IUS will have financial
reporting responsibility. Evidence of control can include funding the software maintenance, exercising access control, and prioritizing enhancements.

6.1.2.5. Capitalized IUS will be accounted for and maintained in the AF IUS APSR, presently the DPAS.

6.2. When to Account for IUS.

6.2.1. When Developing IUS.

6.2.1.1. There are several checkpoints along the developed IUS lifecycle of significance to the timing of the accounting for IUS during development and afterwards. ATP checkpoint 3 (ATP 3) is issued by the Acquiring organization indicating its permission to incur project expenses in conformity with the Acquisitions Strategy. ATP 3 is sometimes referred to as MDA Milestone B, which happens no more than once per Project and per Sub-project, and is issued by the MDA, the software Functional Owner, and the Program Manager (PM). Per DoDI 5000.75, Business Systems Requirements and Acquisition, the development contract award decision point for major automated information systems is equivalent to Milestone B, as described in DoDI 5000.02, Operation of the Defense Acquisition System.

6.2.1.2. ATP 3 indicates that an IUS project under consideration for development has completed its research stage in the software development lifecycle and is approved to move into the development phase. Only during the development phase are construction costs for IUS capitalized and reported IUS in Development for financial reporting purposes. After completion, the finished asset will be reported as "IUS Software" for financial reporting purposes.

6.2.1.3. Allocation of cost to the IUS in Development account stops when the MDA declares that Capability Support ATP has been met, officially ending the development process (end of the development phase for major automated information systems will be the FDD, as described in DoDI 5000.02, Operation of the Defense Acquisition System). Costs that are incurred after development, typically training, maintenance, and support, do not continue to be capitalized as assets, but rather are expensed in the period the cost is incurred.

6.2.1.4. Capitalization at the functionality level is to be used, recognizing that a system could easily have different releases (versions) in different life cycle stages at any one point in time, to provide the same insight and oversight as each capability enters field operation. As such, allocation of cost to the IUS in Development stops at the sprint/release level, rather than at the overall system level. This facilitates tracking to any and all capability as it becomes operational, regardless of the overall system’s life cycle phase.

6.2.1.5. No formal property accountability (i.e., accountable property record) is established until IUS development is completed and functional and is both fielded and operational.

6.2.2. Capitalization of Developed-IUS Development Costs.

6.2.2.1. The AF shall capitalize applicable costs incurred during the software Design/Development and Testing/Implementation (Implementation Phase) phases of the life cycle for IUS. Capitalized costs are accumulated in IUS in Development account until final
user acceptance testing has been successfully completed. Such costs must be limited to those incurred after the following:

6.2.2.1.1. Management authorizes and commits to a computer software project and believes that it is likely that the project will be completed and the software will be used to perform the intended function with an estimated service life of two years or more.

6.2.2.1.2. The completion of conceptual formulation, design, and evaluation of possible software project alternatives (the preliminary design stage).

6.2.2.2. For new Developed IUS software or enhancements, capitalized costs should include the full non-government personnel labor costs (excludes government civilian and military personnel) incurred during the software development stage.

6.2.2.3. Capitalized cost should not include:

6.2.2.3.1. 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.

6.2.2.3.2. Training costs: Post-deployment training costs are to be expensed.

6.2.2.3.3. The costs of minor enhancements: Post-deployment costs resulting from ongoing systems maintenance will NOT be capitalized. They shall be expensed in the period incurred.

Table 6.1. Capitalization of Internal Use Software (IUS) under Waterfall Development Model.
6.2.2.4. The cost of enhancements that add new capabilities to existing IUS (and modules thereof) shall be capitalized when:

6.2.2.4.1. It is likely that the enhancements will result in significant additional capabilities with development cost of the IUS asset over the project development cycle exceeding the capitalization limit (currently $250K or more).

6.2.2.4.2. The enhancements have an expected service life of 2 years or more.

6.2.2.4.3. Significant additional capabilities are modifications to existing IUS that result in additional functionality - that is, modifications to enable the software to perform tasks that it was previously incapable of performing.

6.2.2.5. As stated in FASAB’s SFFAS 10: Accounting for Internal Use Software, paragraph 26, capitalizable enhancements normally require new software specifications and may require a change to all or part of the existing software specifications.

6.2.2.5.1. Examples of major enhancements could include augmenting existing business functions with new features and functions i.e., adding new requirements, developing additional new business functions, and/or adding new functionality and capability.
6.2.2.6. The rules for capitalizing and expensing costs for IUS enhancements should be treated the same as initial developed IUS construction projects, however, they must maintain traceability to the primary IUS asset that is being enhanced.

6.2.3. Capitalization of IUS Development Costs under other IUS Development Models.

While IUS Development may be accomplished using varying development methodologies that use alternative jargon to identify development and non-development. The underlying rules for capitalization and expensing of costs are grounded in common underlying rules that require the capitalization of costs (only) during development and expensing of costs incurred before or after the development phase, regardless of the methodology.

6.2.3.1. Capitalization of Agile Development Cost.

6.2.3.1.1. The Agile software development method is a software development method in which requirements are refined and solutions evolve over phases with collaborations between self-organizing, cross-functional teams. In an agile project, working software is deployed in iterations of typically 1 to 8 weeks in duration, each of which provides a segment of functionality.

6.2.3.1.2. If the numbers of iterations are dependent on the outcomes of multiple processes for a complete function, the cost incurred in these iterations should be grouped together based on the nature of the activities (capital or expensed) and treated as one project.

6.2.3.1.3. Any future incremental releases that result in additional functionality can be treated as an enhancement of the original IUS project and accounted for in accordance.

6.2.3.2. Capitalization of Spiral Development Cost.

6.2.3.2.1. The IUS development phases listed in the Waterfall Development model could be applied to a spiral development project on a process increment basis.

6.2.3.2.2. If an increment developed meets the module or component asset definition, then it could be treated as an individual IUS project and would be accounted for.

6.2.3.2.3. If the number of increments is dependent on the outcomes of multiple spiral processes for a complete function, the cost incurred in these iterations should be grouped together based on the nature of the activities (capital or expensed) and treated as one project for the purposes of recognition, measurement, and disclosure in accordance with FASAB SFFAS 10: Accounting for Internal Use Software.

6.2.3.2.4. Any future incremental releases that result in additional functionality can be treated as an enhancement of the original IUS project and accounted for in accordance with FASAB SFFAS 10: Accounting for IUS.

7. ACCOUNTABILITY PROCESS.

7.1. Acquisition and Procurement Process.

7.1.1. Pre-Contract Award.
7.1.1.1. The Contracting Officer (CO) will ensure the application of uniform CLIN 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. When procuring IUS, AF contracting activities:

a) Ensure that a uniform CLIN and Sub-line numbering (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).

b) Ensure that the appropriate solicitation instructions, provisions contract clauses and CDRLs are included in solicitations and contract awards as applicable.

c) Ensure the CLIN and SLIN structure aligns with the lines of accounting assigned by requiring activities. Table 6.1 details the items required to be separated on CLINs to be capitalized.

d) 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.

e) Ensure contracts for the development of IUS include a listing of all contractor-supplied IUS supplied for use under the contract.

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

7.1.2. Post-Contract Award.

7.1.2.1. When procuring Internal IUS, AF contracting activities:

a) In coordination with the requiring activity review for approval all contractor requests to purchase and/or develop IUS for which the Government will have title.

b) For cost reimbursement contracts requiring financial management and cost reporting, ensure that contractors report approved IUS purchases and/or fabrications as a separate line item.

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

d) Ensure contractors obtain pre-approval for the purchase or development of IUS for which the Government will have title, unless the IUS is a deliverable itemized under the contract or a component of or material for that deliverable as part of the contract award or specifically required within the statement of work.

7.2. IUS Reporting Process.

7.2.1. All Developed IUS that meets capitalization criteria will be accounted for following below process during its development, deployment, enhancement, transfer, and disposal. For specific DPAS processes, refer to the supplemental “DPAS IUS Quick Reference Guide
STANDARD OPERATING PROCEDURE (SOP) FOR INTERNAL USE SOFTWARE (IUS) ACCOUNTABILITY

(QRG)” The QRG will be provided by the SAF/CIO A6SE IT Asset Management (ITAM) office upon request via e-mail until a permanent network link/location can be provided.

7.2.2. Reference Figure 7.1. Accounting Process for Capitalized Developed IUS, for a process view of the IUS reporting process for Developed IUS.
Figure 7.1. Accounting Process for Capitalized Developed IUS.
7.2.3. Accounting of IUS during the Development Phase.

7.2.3.1. Obtain MDA Approval for Software Development (reference Figure 7.1. Accounting Process for Capitalized Developed IUS, step 1).

7.2.3.1.1. There are several checkpoints of significance along the developed IUS lifecycle. One of which is the ATP. At ATP 3, an ADM is issued by the MDA indicating permission to begin development activity, and incurring project expenses in conformity with the Acquisitions Strategy. This happens no more than once per Project and per Sub-project, and is issued by the MDA, the software Functional Owner, and the PM.

7.2.3.1.2. The PM sends a copy of the ADM signed at ATP 3 to the Functional Support Team, or otherwise communicates the attainment to the ATP 3 to DPAS Project Administrator for project creation in DPAS (see step 1 in Figure 7.1. Accounting Process for Capitalized Developed IUS).

7.2.3.1.3. An Acquisitions Strategy document is required to support the Authority to Proceed (ATP) 3. The MDA reviews and confirms that valuation attested by the PM/Asset Manager (AM) is accurate and supportable information and documentation.

7.2.3.1.4. The significance of the ATP is that it signals the authority to move ahead with the construction (development) phase of the IUS asset's Software Development Lifecycle (SDLC). It is upon successful completion of this event, (evidenced by an ATP 3 ADM), that project costs no longer are to be expensed, and are to begin accumulation in IUS in Development account within a DPAS project.

7.2.4. Establish IUS in Development Record in DPAS (reference Figure 7.1. Accounting Process for Capitalized Developed IUS, step 4).

7.2.4.1. Refer to Section 8 of this SOP on how to onboard DPAS for IUS in Development action.

7.2.4.2. Additional DPAS IUS accountability desktop guidance will also be provided upon request from usaf.pentagon.rsrcmgmt.mbx.saf-cio-a6-itam-workflow@mail.mil

7.2.4.3. After MDA approval has been given for software development, PM's functional support personnel create a new IUS in Development record in DPAS to enable phase capability support.

7.2.4.4. Within 3 days of the receipt of ATP 3 ADM, the PMO centralized acquisition functional support team or DPAS Project Administrator creates either a new IUS in Development Project or sub-Project in DPAS.

7.2.4.5. PM/AM collects, maintains, and uploads all KSD into DPAS in support of asset existence and capital valuation during asset’s development phase.

7.2.4.6. Creation is sufficient to allow the entry and posting of Project and sub-Project costs to the IUS in Development Project, to capture development costs and ultimately trigger
STANDARD OPERATING PROCEDURE (SOP) FOR INTERNAL USE SOFTWARE (IUS) ACCOUNTABILITY

completion of the Developed IUS asset. The Project or sub-Project in DPAS is identified as an IUS asset under construction.

7.2.4.7. PMO/COR, in the DPAS role of APO for the IUS in Development asset, collects contributing cost data and supporting KSDs and updates IUS in Development records in DPAS within 3 days of invoice receipt.

7.2.4.8. Contributing costs include items such as:

a) IUS Development Project and Sub-Project expenses.

b) Vendor labor/development costs.

c) COTS software used exclusively in the development of IUS.

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

e) Cloud Service Provider service and user fees used to support lower level platform and infrastructure environments used exclusively in the development of IUS

7.2.5. Capture IUS Costs during Development (reference Figure 7.1. Accounting Process for Capitalized Developed IUS, steps 5, 9, 11, and 12).

7.2.5.1. Upon receiving invoices, the PMO/COR validates that the Invoice received conforms to the terms of the contract regarding Developed IUS CLIN and CDRL identifications. The COR plays the role of inspector and acceptor. The COR will do the following in determining whether to approve or reject invoice in Invoicing, Receipt, Acceptance and Property Transfer (iRAPT).

a) Ensure that contract data requirements list (CDRL) information, as defined during contracting and required to be reported by the vendor, is included the invoiced materials, as applicable.

b) Ensure that CLIN information, as defined during contracting and required to be reported by the vendor, is included the invoiced materials, as applicable.

c) Ensure that other elements of the contract are complete and accurate and that work being billed on the invoices was actually performed during the billing period.

7.2.5.2. If Vendor-provided invoice does not provide the applicable IUS CLIN, COR or PM notifies Vendor of invalid invoice due to missing or incorrect CLIN or CDRLs, for services performed in part or in whole to develop IUS. Vendor is requested to correct invoice data and resubmit for processing.

7.2.5.3. Within 3 days of receiving an acceptable invoice, PMO COR Support Element Personnel enter valid developed IUS cost data and upload supporting KSD into Construction-in-Progress records established in DPAS.

7.2.6. Obtain MDA approval of software limited or full deployment in an operational environment (reference Figure 7.1. Accounting Process for Capitalized Developed IUS, steps 13 and 14).
7.2.6.1. MDA determines when and whether 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 communicates the approval to field to the PMO. This Decision Memo also serves as the evidence for:

a) Discontinuance of further capitalization of development costs for that specific functionality in the IUS in Development account.

b) Inactivation of reporting of that functionality’s IUS in Development account balance.

c) Creation of a new IUS asset in DPAS, or for subsequent functions, updating the existing DPAS account of the additional functionality and its associated costs.

7.2.7. Recognize IUS Asset in DPAS and Relieve IUS in Development account (reference Figure 7.1. Accounting Process for Capitalized Developed IUS, steps 15 and 16).

An ADM is used to declare the achievement of Capability Support ATP, which denotes completion of the IUS development activity. Within 7 days of attaining the ADM, but within the same reporting period if less than 7 days, PM or AC PMO updates status of IUS in Development record in DPAS to record that the IUS development for this Project or sub-Project is complete. This action is reflected in DPAS by updating the Developed IUS record in DPAS to create a transfer order that transfers the developed IUS asset from IUS in Development to a completed IUS asset in DPAS. The transfer results in the creation of a completed IUS asset in DPAS in Pending status. Through DPAS automation, the Receipt of the transfer completes the transfer process in DPAS resulting in:

a) Discontinuing further capitalization of development costs for that increment.

b) Inactivation of reporting of IUS in Development balance.

c) Creation of a new IUS asset in DPAS.

d) Defaulting the IUS asset’s place in service date to be the same as the date the asset transfer was received (but able to be updated to reflect actual date).

8. DPAS ON-BOARDING.

8.1. DPAS User Account Creation.

8.1.1. Email SAF/CIO A6SE IT Asset Management (ITAM) Office at: usaf.pentagon.rsrmgmt.mbx.saf-cio-a6-itam-workflow@mail.mil to request DPAS user account(s).

8.1.2. SAF/CIO A6SE ITAM Office will respond with all applicable information and on-boarding package required to create user account(s) based on user's role in IUS accountability process.

8.1.3. Once SAF/CIO A6SE ITAM Office has received required information and documentation, the appropriate user account(s) will be created in DPAS.

8.2. Organizational Account Creation in DPAS.
8.2.1. All Major Commands (MAJCOM), Direct Reporting Units (DRU), and 2-letter organizations are required to record their assets under their applicable DPAS organizational accounts.

8.2.2. E-mail SAF/CIO A6SE ITAM Office at: usaf.pentagon.rsrcmgmt.mbx.saf-cio-a6-itam-workflow@mail.mil to request an organizational account in DPAS.

8.2.3. SAF/CIO A6SE ITAM Office will provide necessary information/documentation to create the organizational account based on the requestor's role.

8.2.4. Upon receipt of required information and documentation, SAF/CIO A6SE ITAM Office will create the organizational account in DPAS.

8.3. DPAS training.

8.3.1. DPAS will provide training, based on the user's assigned role, on the DPAS training website: https://dpaselearning.golearnportal.org/login/index.php.

8.3.2. E-mail the SAF/CIO A6SE IT Asset Management Office (ITAM) Office at: usaf.pentagon.rsrcmgmt.mbx.saf-cio-a6-itam-workflow@mail.mil for additional support.

8.3.3. Additional IUS DPAS training is available from the SAF/CIO A6SE ITAM Office via a step-by-step DPAS IUS Quick Reference Guide (QRG) and can be provided upon request.
STANDARD OPERATING PROCEDURE (SOP) FOR INTERNAL USE SOFTWARE (IUS) ACCOUNTABILITY

Appendix A
INTERNAL USE SOFTWARE (IUS) ASSET DETERMINATION

START

Is it Software?

NO

YES

Embedded in Weapon?

NO

YES

Sw Integrated Into HW?

NO

Determine System Type

OUTSOURCED IT?

YES

NOT IUS

NO

SW Delivered as a Service?

YES

All Other Systems

ACCOUNT AS IUS
## Appendix B

### EXAMPLES OF INTERNAL USE SOFTWARE (IUS)

Table B.1. Examples of IUS.

<table>
<thead>
<tr>
<th>Definition</th>
<th>IUS</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Control Software</strong></td>
<td>NO</td>
<td>Common Access Card (CAC) Reader Software</td>
</tr>
<tr>
<td>This type of software, which is external to the operating system,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>provides a means of specifying who has access to a system and the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>specific capabilities authorized users are granted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Application Software</strong></td>
<td>YES</td>
<td>Microsoft (MS)</td>
</tr>
<tr>
<td>A software program that performs a specific function directly for a</td>
<td></td>
<td>Excel, Adobe Photoshop, MS Project, MS Visio</td>
</tr>
<tr>
<td>user and can be executed without access to system control, monitoring,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>or administrative privileges.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cloud, Public Infrastructure</strong></td>
<td>NO</td>
<td>Amazon Web Services (AWS), Azure</td>
</tr>
<tr>
<td>A cloud-based environment that is generally external to the Department</td>
<td></td>
<td></td>
</tr>
<tr>
<td>with infrastructure owned and managed by a third party. Public cloud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>services are generally subscription based.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cloud, Private</strong></td>
<td>YES</td>
<td>Army Private Cloud Enterprise (APCE), Redstone</td>
</tr>
<tr>
<td>An on-premises cloud-based environment that is generally internal to the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Department and used solely by the AF.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Database Management Systems</strong></td>
<td>YES</td>
<td>Oracle</td>
</tr>
<tr>
<td>Commercial software that integrates business information flowing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>through the Component. Enterprise Resource Planning (ERP) systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>contain functional modules (e.g., financial, accounting, human</td>
<td></td>
<td></td>
</tr>
<tr>
<td>resources, supply chain, and customer information) that are integrated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>within the core system or interfaced to external systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Enterprise Resource Planning System</strong></td>
<td>YES</td>
<td>Defense Enterprise Accounting and Management System (DEAMS)</td>
</tr>
<tr>
<td>Commercial software that integrates business information flowing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>through contain functional modules (e.g., financial, accounting,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>human resources, supply chain, and customer information) that are</td>
<td></td>
<td></td>
</tr>
<tr>
<td>integrated within the core system or interfaced to external systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Firmware</strong></td>
<td>NO</td>
<td>Radar system software, lathe software</td>
</tr>
<tr>
<td>A program recorded in permanent or semi-permanent computer memory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firmware should be capitalized as part of equipment it is integrated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>into.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Freeware/Open Source Software</strong></td>
<td>NO</td>
<td>Internet Explorer (IE), Chrome, Firefox, MS Paint</td>
</tr>
<tr>
<td>Software that is offered at no cost.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## STANDARD OPERATING PROCEDURE (SOP) FOR INTERNAL USE SOFTWARE (IUS) ACCOUNTABILITY

### Software Integrated into Hardware

<table>
<thead>
<tr>
<th>Description</th>
<th>YES/NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software that is integrated into the physical components of IT, including into servers, computers, peripheral devices, disks, scanners, switches, and other IT equipment.</td>
<td>NO</td>
</tr>
<tr>
<td>Computer Operating Systems</td>
<td></td>
</tr>
</tbody>
</table>

### Software License – Annual

<table>
<thead>
<tr>
<th>Description</th>
<th>YES/NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>A software license that must be renewed annually to continue using the software (with the expectation that the AF will renew the license)</td>
<td>YES</td>
</tr>
<tr>
<td>MS Lync, VMWare, vSphere</td>
<td></td>
</tr>
</tbody>
</table>

### Software License – Enterprise

<table>
<thead>
<tr>
<th>Description</th>
<th>YES/NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>A license that allows use of the software throughout an organization or for a specified number of users.</td>
<td>YES</td>
</tr>
<tr>
<td>MS Office, Oracle</td>
<td></td>
</tr>
</tbody>
</table>

### Software License – Perpetual

<table>
<thead>
<tr>
<th>Description</th>
<th>YES/NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>A software license that gives the Department the right to use the software in perpetuity.</td>
<td>YES</td>
</tr>
<tr>
<td>Systems, Applications and Products (SAP) Crystal Reports</td>
<td></td>
</tr>
</tbody>
</table>

### Middleware

<table>
<thead>
<tr>
<th>Description</th>
<th>YES/NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer software that provides services to software applications beyond those available from the operating system.</td>
<td>YES</td>
</tr>
<tr>
<td>AF system to system interfaces</td>
<td></td>
</tr>
</tbody>
</table>

### Portal

<table>
<thead>
<tr>
<th>Description</th>
<th>YES/NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web-based application that provides personalization, single sign-on, and content aggregation from different sources, and hosts the presentation layer of information systems.</td>
<td>YES</td>
</tr>
<tr>
<td>AF Portal, Customized Microsoft (MS) SharePoint Sites</td>
<td></td>
</tr>
</tbody>
</table>

### Simulation Software

<table>
<thead>
<tr>
<th>Description</th>
<th>YES/NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>NO</td>
</tr>
<tr>
<td>Flight Training Software</td>
<td></td>
</tr>
</tbody>
</table>

### Operating System

<table>
<thead>
<tr>
<th>Description</th>
<th>YES/NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>NO</td>
</tr>
<tr>
<td>Windows, Linux, iOS</td>
<td></td>
</tr>
</tbody>
</table>

### System/IT System

<table>
<thead>
<tr>
<th>Description</th>
<th>YES/NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>The term &quot;system&quot; 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 &quot;system&quot;.</td>
<td>YES</td>
</tr>
<tr>
<td>IT Investment Portfolio System (ITIPS), Defense Enterprise Accounting and Management System (DEAMS)</td>
<td></td>
</tr>
<tr>
<td><strong>Utility Program</strong></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>---</td>
</tr>
<tr>
<td>System software designed to perform a particular function or system maintenance.</td>
<td>NO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Web Application</strong></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>An application that is accessed via the web over a network.</td>
<td>YES</td>
<td>Webmail</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Audio/Visual Equipment</strong></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio and Visual equipment have generally integrated software which is not IUS.</td>
<td>NO</td>
<td>VTC, CISCO phone equipment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Outsourced Information Technology (IT)</strong></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Software capabilities provided by non-AF entities and using COTS IUS licenses owned by those non-AF entities.</td>
<td>NO</td>
<td>Cloud services</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Software as a Service (SaaS)</strong></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>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).</td>
<td>NO</td>
<td>Microsoft 365</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Network</strong></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Normally network consists of routers and switches which utilizes integrated software and do not qualify as IUS.</td>
<td>NO</td>
<td>Secret Internet Protocol (IP) Router Network (SIPRNet), Non-classified Internet Protocol (IP) Router Network (NIPRNet)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Host / Network Monitoring Software</strong></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Standalone host and network monitoring software other than those integrated into switches and routers.</td>
<td>YES</td>
<td>Microsoft System Center Configuration Manager (SCCM), Host Based Security System (HBSS), Tanium, SolarWinds</td>
</tr>
</tbody>
</table>
STANDARD OPERATING PROCEDURE (SOP) FOR INTERNAL USE SOFTWARE (IUS) ACCOUNTABILITY

<table>
<thead>
<tr>
<th>Weapon System (Military Equipment)</th>
<th>NO</th>
<th>AF weapons and weapon systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>In accordance with DoD FMR 7000.14-R, Chapter 6, section 060209, IUS (Account 1830); “IUS does not include software (SW) embedded in military equipment (weapons system) nor does it include SW used in Special Test Equipment. To further clarify, IUS embedded within a military equipment asset is not solely excluded upon classification as such. The SW/IUS must be necessary to operate the equipment. If, upon removal of the SW/IUS, the system will not operate as intended, it shall be considered non-IUS. If the SW/IUS and military equipment can still function as intended when separated, then it is considered SW/IUS and must be accountable.”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>In addition: Chapter 6, section 060103 A.1 -2: 2. These weapons systems are referred to as military equipment. In addition to the requirements of 060103.A.1 (a through d), military equipment items are intended to be used by the Armed Forces to carry out battlefield missions, are referred to as military equipment. Examples include: combat aircraft, pods, combat ships, support ships, satellites, and combat vehicles. Additional guidance follows: a. Military equipment does not ordinarily lose its identity or become a component part of another article; and is available for the use of the reporting entity for its intended purpose. b. Intangible assets, such as SW, are not considered military equipment; however, the cost of the intangible asset shall be included in the cost of the related military equipment. c. Military equipment assets are generally functionally complete and should be valued based on the cost of the final assembly, including the cost of the embedded items.”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software/IUS supporting weapons systems which are integrated and unable to be withdrawn from equipment without breaking both assets.</td>
<td>YES</td>
<td>AF weapons system</td>
</tr>
</tbody>
</table>

**Exception:** Information systems supporting weapons systems will be accounted as IUS.
STANDARD OPERATING PROCEDURE (SOP) FOR INTERNAL USE SOFTWARE (IUS) ACCOUNTABILITY

Appendix C

KEY SUPPORTING DOCUMENTS IN SUPPORT OF IUS AUDITABILITY

Authority to Proceed – Acquisition Authority Decision Memo

Authority to Proceed – Capability Support Authority Decision Memo

Contracts, including Statements of Work (SOW)

Date Placed In Service Documentation

Declaration of Excess

Disposal Disposition

Documentation supporting allocation methodology for direct labor costs and distribution for indirect labor costs and overhead costs

Documentation supporting the purchase of COTS IUS licenses and specific costs incurred for implementation

Documentation supporting the amounts paid to contractor for design, programming, installation, and implementation of new software or to modify existing software plus costs incurred for implementation

Impairment Determination Documentation

Invoices

Military Interdepartmental Purchase Requests (MIPR)

Obligating Documents

Purchase Orders (PO)

Received Reports

Reimbursable Agreements

Requests for Transfer of Property

Time Sheets

Useful Life Estimate Documentation

Work Orders
Appendix D

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

HR 1232, Federal IT Acquisition Reform Act (FITARA), September 18, 2014


Federal Acquisition Regulation (FAR), Part 7 - Acquisition Planning, August 22, 2018

Memorandum, Office of the Under Secretary of Defense, Deputy Chief Financial Officer, Strategy for IUS Audit Readiness, September 30, 2015

Defense Federal Acquisition Regulation Supplement (DFARS), Part 207 - Acquisition Plans, October 1, 2018

Defense Federal Acquisition Regulation System (DFARS) Procedures, Guidance, and Information (PGI), 204.7103 - Contract Line Items, May 30, 2018

AF Federal Acquisition Regulation Supplement (AFFARS), Part 5307 - Acquisition Planning, May 25, 2018

DoDI 5000.02, Operation of the Defense Acquisition System, January 7, 2015

DoDI 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property, 27 April 2017
STANDARD OPERATING PROCEDURE (SOP) FOR INTERNAL USE SOFTWARE (IUS) ACCOUNTABILITY

DoDI 5000.75, Business Systems Requirements and Acquisition, February 2, 2017
DoDI 5000.76, Accountability and Management of IUS March 2, 2017
DoD FMR 7000.14-R, Volume 4, Chapter 6, Property, Plant and Equipment, January 2016
DoD FMR 7000.14-R, Volume 4, Chapter 27, Internal Use Software, August 2018
Financial Improvement and Audit Readiness (FIAR) Guidance, Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, April 2016
AF Manual (AFMAN) 17-1203, ITAM, May 18, 2018

Prescribed Forms
No forms are prescribed by this publication

Adopted Forms
DD Form 3041, APSR Requirements Checklist for IUS, March 2017
STANDARD OPERATING PROCEDURE (SOP) FOR
INTERNAL USE SOFTWARE (IUS) ACCOUNTABILITY

Appendix E

ABBREVIATIONS

AC - Asset Custodian
ADM - Acquisition Decision Memo
AF - Air Force
APO - Accountable Property Officer
APSR - Accountable Property System of Record
ATP - Authority to Proceed
CDRL - Contract Data Requirements List
CLIN - Contract Line Item Number
CO - Contracting Officer
COR - Contracting Officer Representative
COTS - Commercial off-the-shelf
DoD - Department of Defense
DoD FMR - Department of Defense Financial Management Regulation
DoDI - DoD Instruction
DPAS - Defense Property Accountability System
FASAB - Federal Accounting Standards Advisory Board
FDD - Full Deployment Decision
GOTS - Government Off-the-Shelf
IT - Information Technology
IUS - Internal Use Software
KSD - Key Supporting Document
MDA - Milestone Decision Authority
PM - Program Manager
PMO - Program Management Office
PP&E - Property, Plant, & Equipment
SAF/AQ - Secretary of the Air Force/Acquisition
SAF/CIO A6 - Secretary of the Air Force, Chief, Information Dominance & Chief Information Officer
SAF/FM - Secretary of the Air Force/Financial Management
STANDARD OPERATING PROCEDURE (SOP) FOR
INTERNAL USE SOFTWARE (IUS) ACCOUNTABILITY

SFFAS - Statement of Federal Financial Accounting Standards

SOP - Standard Operating Procedures
Acceptance - As defined in DoDI 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property.

Accountability - As defined in DoDI 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property.

Accountable property - As defined in DoDI 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property.

Accountable Property Officer (APO) - As defined in DoDI 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property.

Accountable property record - As defined in DoDI 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property.

Accountable Property System of Record (APSR) - As defined in 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property. For this issuance, APSR refers specifically to IUS and IUS requirements.

Amortization - The process of allocating the expense of an intangible asset (such as IUS) over its estimated useful life.

Bulk license purchase - A one-time purchase against one particular purchase order or delivery order for the acquisition of a quantity of identical items, where the total monetary value of the one-time acquisition is greater than or equal to the capitalization threshold and the IUS being purchased has a license term that is greater than or equal to 2 years or has a perpetual software license. The one-time acquisitions of IUS that fail to meet or exceed the capitalization threshold or have a license term of fewer than 2 years will not be considered for bulk license purchase accounting treatment. Accounting guidance is located in Volume 4 of Department of Defense Financial Management Regulation (DoDFMR) 7000.14-R.

Capitalized IUS - IUS costs that are accounted for as purchases of assets rather than as expense. IUS cost must be accumulated in IUS in Development account during the development phase for developed IUS or as an IUS asset for finished IUS. IUS must meet or exceed the capitalization threshold. Capitalized IUS must be maintained in an APSR, amortized, and reported annually on the Department of Defense (DoD) balance sheets and accompanying note 10.

Commercial services - Services provided by private vendors.

Commercial off-the-shelf (COTS) Software - Software developed, tested, and sold by commercial companies to the general public. This software meets operational requirements without modification or alteration to perform on a DOD network or computer. Examples include word processors, databases, application generation, drawing, compiler, graphics, communications, and training software.

Contractor-developed software - Software that a federal entity is paying a contractor to design, program, install, and implement, including new software and the modification of existing or purchased software.
STANDARD OPERATING PROCEDURE (SOP) FOR
INTERNAL USE SOFTWARE (IUS) ACCOUNTABILITY

Defense Property Accountability System (DPAS) - DPAS is a Department of Defense (DoD) property management system. It is the APSR for over 32 DoD Agencies and Military Services. It contains four modules; Property Accountability, Maintenance & Utilization, Warehouse Management, and Materiel Management.

Full Operational Capability (FOC) - FOC is when a system is delivered to a user and they have the ability to fully employ and maintain it to meet an operational need. The mission capabilities of an FOC system are defined in a system’s Capability Development Document (CDD) and Capability Production Document (CPD).

Government Off-the-Shelf (GOTS) Software - A software and/or hardware product that is developed by the technical staff of a Government organization for use by the U.S. Government. GOTS software and hardware may be developed by an external entity, with specification from the Government organization to meet a specific Government purpose, and can normally be shared among Federal agencies without additional cost. GOTS products and systems are not commercially available to the general public. Sales and distribution of GOTS products and systems are controlled by the Government.

Initial Operating Capability (IOC) - IOC is a point in time during the Production & Deployment (PD) Phase where a system can meet the minimum operational (Threshold and Objective) capabilities for a user’s stated need. The operational capability consists of support, training, logistics, and system interoperability within the Department of Defense (DoD) operational environment. IOC is a good gauging point to see if there are any refinements needs before proceeding to Full Operational Capability (FOC).

Interagency services - Services provided by one Department of Defense (DoD) organization to other DoD or federal organizations that are outside of the provider’s organizational boundaries.

Internal Use Software - Refer to Chapter 2

Intra-agency service - Services provided within the boundaries of a Department of Defense (DoD) organization to that organization’s internal units.

Managerial system - A system used to manage IT and information system assets, including National Security Systems. It is an authoritative source of information regarding assets, asset usage, management support, portfolio support, or as defined in the system documentation. It supports the tracking and management of the Department of Defense’s (DoD) existing processes for IT portfolio management; acquisition and procurement management; and financial management (i.e., planning, programming, budgeting, and execution).

National Stock Number - As defined in Department of DoDI 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property.

Parent system - A system comprised of multiple applications, modules, or other germane units which may be separately identified (e.g., system sub-systems). For example, system ABC is a legacy system that was subsequently migrated into system DEF. System DEF is the parent; system ABC is the system sub-system.

Physical inventory - As defined in DoDI 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property.

Property loss - As defined in DoDI 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property. For IUS, loss may include corruption due to virus, accidental destruction
STANDARD OPERATING PROCEDURE (SOP) FOR INTERNAL USE SOFTWARE (IUS) ACCOUNTABILITY

of installation media, loss of license information, or other incidents germane to software becoming unusable.

Reconciliation - As defined in DoDI 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property.

SNaP-IT - The electronic system used by the Department of Defense Chief Information Officer (DoD CIO) to collect IT Budget and Cyberspace Operations Budget data and generate reports mandated by the Office of Management and Budget (OMB) and Congress.

System sub-systems - Applications, modules, or other germane units collectively operating under a parent system. System sub-systems may have a DoD Software Unique Identifier, Defense IT Portfolio Repository (DITPR) number, or other assigned identifier. For example, system ABC is a legacy system that was subsequently migrated into system DEF. System DEF is the parent; system ABC is the system sub-system. System ABC may have had a DITPR number assigned prior to migration.

Useful life - The period during which an asset is expected to be usable for the purpose it was acquired. The useful life of IUS is stated 2-5, or 10 years for IUS.
This Air Force Manual (AFMAN) implements Executive Order (E.O.) 13103, Computer Software Piracy and Air Force Policy Directives (AFPD) 17-1, Information Dominance Governance and Management and supports AFPD 17-2, Cyberspace Operations, and AFPD 10-6, Capabilities Requirements Development. This AFMAN provides the overarching guidance and direction for managing IT hardware and software. The hardware management guidance identifies responsibilities for supporting Air Force (AF) IT hardware (IT assets). The software management guidance identifies responsibilities for management of commercial off-the-shelf (COTS) software. This AFMAN applies to the Air National Guard (ANG) and the Air Force Reserve (AFR) unless indicated otherwise. One or more paragraphs of this AFMAN may not apply to non-AF-managed joint service systems. These paragraphs are marked as follows: (NOT APPLICABLE TO NON-AF-MANAGED JOINT SERVICE SYSTEMS). The authorities to waive wing/unit level requirements in this publication are identified with a Tier (“T-0, T-1, T-2, and T-3”) number following the compliance statement. See AFI 33-360, Publications and Forms Management, Table 1.1., for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or for non-tiered compliance items, the local commander. Send recommended changes or comments, through appropriate command channels, to Enterprise IT Integration Division (SAF/CIO A6SE) using AF Form 847, Recommendation for Change of Publication. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, Management of Records, and the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). The use of the name or mark of any specific manufacturer, commercial product, commodity, or
service in this publication does not imply endorsement by the Air Force. See Attachment 1 for a glossary of references and supporting information.

**SUMMARY OF CHANGES**

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

**Chapter 1— IT ASSET MANAGEMENT**

1.1. Overview

1.2. Roles and Responsibilities. Figure 1.1

Figure 1.1. Information Technology Asset Management Roles and Responsibilities Overview

**Chapter 2— HARDWARE ASSET MANAGEMENT**

2.1. Accountability of Information Technology (IT) Hardware Assets.

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

Table 2.1. End User Device Refresh Rate.

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

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

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

**Chapter 3— SOFTWARE ASSET MANAGEMENT**


3.2. General Guidelines for Acquisition of Software.

3.3. Management of Non-Enterprise Commercial Software.

3.4. Management of Enterprise Software.

3.5. Internal Use Software (IUS) Accountability.

Table 3.1. Internal Use Software (IUS) Capitalization Cost Determination.
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 25
Attachment 2—DESIGNATED ACCOUNTABLE PROPERTY SYSTEM OF RECORD (APSR) GUIDANCE 33
Attachment 3—INFORMATION TECHNOLOGY (IT) HARDWARE ENTERPRISE INVENTORY PLAN 35
Chapter 1

IT ASSET MANAGEMENT

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

1.2. Roles and Responsibilities. Figure 1.1 below represents an overview of those Information Technology Asset Management (ITAM) roles and responsibilities from the AF to the organizational level.
1.2.1. Secretary of the Air Force, Chief, Information Dominance & Chief Information Officer (SAF/CIO A6).

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

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

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

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

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

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

1.2.1.7. Surveys, consolidates, validates, and tracks all MAJCOM, Field Operating Agency (FOA), and Direct Reporting Unit (DRU) requirements for potential AF enterprise software licenses for COTS software.
1.2.1.8. Recommends candidate software products for potential AF-wide or Department of Defense (DoD)-wide licensing to the Air Force Materiel Command (AFMC) product center designated with the responsibility for procurement of enterprise licenses as the purchasing agent.

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

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

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

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

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

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

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

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

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

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

   1.2.4.1. Serves as lead for implementation of Information Technology Asset Management (ITAM).
1.2.4.2. Publishes software entitlesments, implementation and ITAM account inventory metrics.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.2.8. MAJCOM, DRU, FOA, or Equivalent:

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

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

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

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

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

1.2.9.1.1. Not be the ECO in the same command according to DoD Financial Management Regulation (DoDFMR) 7000.14-R, Volume 3, Chapter 8, Managers’ Internal Control Program Procedures, (T-0).

1.2.9.2. Maintain the list of designated ECOs.

1.2.9.3. Ensure compliance with this AFMAN across their portfolio.

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

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

1.2.9.6. Complete additional training as directed by the AFECO.

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

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

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

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

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

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

1.2.11.2.1. Appoint at least one primary and one alternate ECO, document acknowledgement of duties with handwritten or digital signatures, and provide a copy to the MECO, (T-1).
1.2.11.2.2. Ensure the designated APSR inventory provides accountability of all IT hardware assets, IAW Chapter 2, (T-1).

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

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

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

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

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

1.2.12. Equipment Control Officer (ECO):

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

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

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

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

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

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

1.2.12.2.3. Provides Unit APOs with asset labels.

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

1.2.12.3. Completes additional training as directed by the MECO.

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

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

1.2.13.1. Ensure annual inventories are conducted for all non-enterprise software licenses for all organizations under BSLM purview, (T-0).
1.2.13.2. Collect an annual baseline of an inventory for all non-enterprise software licenses, (T-1).

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

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


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

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

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

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

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

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

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

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

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

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

1.2.14.9. Identify enterprise software license requirements and any management training requirements not covered in existing courses to the BSLM (or equivalents) for annual consolidation, (T-3).
Chapter 2

HARDWARE ASSET MANAGEMENT

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

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

2.1.1.1. Accountable Property Record (APR) Process.

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

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

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

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

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

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

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

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

2.1.1.2. Accountability Record (AR) Process.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.2.1.2. The MAJCOM/A6s (or equivalents) may approve a QEB or DPI waiver via AFWay process, however MAJCOMs and Program Offices must use either AFWay-approved vendors or a NETCENTS-2 contract to meet their mission requirements, (T-1).
2.2.2. Ensure complete information is provided for shipping labels for ordered equipment. Obtain confirmation that procurement officials specify, as a contractual requirement, that “Ship To” and “Mark For” information is detailed on the shipping labels. This will alleviate problems with the receipt and acceptance processing of new hardware assets.

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

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

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

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

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop</td>
<td>5 years</td>
</tr>
<tr>
<td>Laptop</td>
<td>4 years</td>
</tr>
<tr>
<td>Tablet</td>
<td>4 years</td>
</tr>
<tr>
<td>Cell Phone</td>
<td>2 years</td>
</tr>
<tr>
<td>Printer: Stand-alone</td>
<td>5 years</td>
</tr>
<tr>
<td>Printer: Multi-Functional Device</td>
<td>5 years</td>
</tr>
</tbody>
</table>

*Based on average warranties

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

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

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

2.3.1.1.1. The ECO or supporting personnel will enter newly received IT assets into the designated APSR. When received by anyone other than the ECO, the ECO will be notified of the asset(s) delivery. The asset will be secured and the asset(s) key supporting documentation (KSD) will be provided for inclusion to the APSR within 7 working days of receipt and acceptance. Capital assets must be recorded by the end of the month or within 7 calendar days, whichever is sooner, (T-0). Prior ECO approval is required when deviating from the standard ECO asset(s) delivery process.
2.3.1.2. Ensure unique asset identification is established for each item according to Serialized Item Management (SIM) and Item Unique Identification (IUID) guidance in AFI 63-101/20-101, Integrated Life Cycle Management, (T-0).

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

2.4.1. Inventory.

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

2.4.2. Inventory Frequency.

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

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

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

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

2.4.4. Reports of Survey.

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

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


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

2.4.4.4. Contractor Guidance.

2.4.4.4.1. Establish the extent of contractor liability in the provisions of the applicable contract’s government property clause according to AFI 23-111, Management of Government Property in Possession of the Air Force.
2.5. Disposition of Information Technology (IT) Hardware Assets.

2.5.1. **Transfer.**

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

2.5.2. **Disposal.**

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

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

2.5.2.3. Prior to disposal, the asset will have:

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

2.5.2.5. All applicable documentation related to the disposal process completed and signed, (T-0).
Chapter 3
SOFTWARE ASSET MANAGEMENT


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

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

3.1.3. This chapter has been divided into 3 sections:

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

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

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

3.2. General Guidelines for Acquisition of Software.

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

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

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

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

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

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

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

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

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

3.3.1. **Receipt and Acceptance.**

3.3.1.1. Proof of software purchase (i.e. purchase order, receipt, shipping order, etc.) will be kept on file with the BSLM as a component of the asset record, (T-0).

3.3.1.2. Proof of government ownership of software (End User License Agreement, contract clauses, etc.) will be kept on file with the BSLM as a component of the asset record, (T-0).

3.3.1.3. Proof of software purchase and proof of government rights to the software will be retained regardless of dollar value of the purchase, (T-0).

3.3.1.4. The asset record will be created in the designated management system or Accountable Property System of Record (APSR) within 7 working days of receipt and acceptance by the government or by the end of the calendar month, whichever is shorter, (T-0).

3.3.2. **General Management of Use.**

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

3.3.3. **Inventory of Non-Enterprise Software.**

3.3.3.1. Organizations will inventory all licensed software annually and, if available utilize auto-discovery tools, to track and report implemented software and license information, (T-0).

3.3.3.2. The Unit APO will certify the annual inventory with a handwritten or digital signature indicating completion of the inventory and submit to the BSLM (or equivalents), (T-0).

3.3.4. **Management of Legal Use.**

3.3.4.1. Organizations will audit all systems to ensure no illegal or unauthorized copies of software are installed. Sampling procedures may be used if active inventoring/auto discovery systems are available, (T-0).

3.3.4.2. Automated tools should be used to the maximum extent possible for tracking software installed on the base network where applicable.

3.3.5. **Managing Software Reuse.**

3.3.5.1. Redistribution of excess or superseded software may occur if it:

3.3.5.1.1. Is permitted under the license agreement or upgrade policy for that software.

3.3.5.1.2. Is not classified.

3.3.5.1.3. Did not provide direct security protection to systems that processed classified information.
3.3.5.1.4. Is not directly related to or associated with a weapon system, intelligence system, command and control system, communications system, or tactical system.
3.3.5.1.5. Still operates as intended.
3.3.5.2. The asset record, and all documentation associated with it, must be transferred to the gaining organization along with the asset, (T-0).

3.3.6. **Managing Software Disposal.**

3.3.6.1. Dispose of excess or superseded software not redistributed by one of the following methods and according to license agreements:

3.3.6.1.1. Return the software package (distribution media, manuals, etc.) to the company that developed the software.
3.3.6.1.2. Destroy the software and license keys according to the provisions of the licensing agreement.

3.3.6.2. Document the method of destruction to establish an audit trail, (T-0).

3.4. **Management of Enterprise Software.**

3.4.1. At a minimum:

3.4.1.1. Legal use of enterprise licenses will be monitored by the Base Software License Manager (BSLM) to ensure usage does not exceed quantities purchased, (T-0).
3.4.1.2. The BSLM will perform and annual inventory of Enterprise software licenses reconcile them against contract information to maintain accountability of what the government has purchased as well as to ensure adherence to legal use per contract terms, (T-1).

3.5. **Internal Use Software (IUS) Accountability.**

3.5.1. **Description.**

3.5.1.1. IUS is:

3.5.1.1.1. Acquired or developed to meet internal or operational needs.
3.5.1.1.2. A stand-alone application, or the combined software components of an Information Technology (IT) system that can consist of multiple applications, modules, or other software components integrated and used to fulfill internal or operational need.
3.5.1.1.3. Used to operate the programs (e.g. financial and administrative software).
3.5.1.1.4. Used to produce goods and provide services (e.g. maintenance work order management).
3.5.1.1.5. Developed to or obtained for internal use and subsequently provided to other federal entities with or without reimbursement.

3.5.1.2. IUS is not:

3.5.1.2.1. Software that is integrated into and necessary to operate equipment rather than perform an application (i.e., an operating system).
3.5.2. **General Accountability.** Accountability of Internal Use Software (IUS) will be:

3.5.2.1. Established and maintained:

3.5.2.1.1. At the end of the development phase for government- or contractor-developed IUS, (T-0).

3.5.2.1.2. Upon government acceptance of commercial off-the-shelf (COTS) IUS, (T-0).

3.5.2.1.3. Upon the completed transfer to another unit/organization within the Air Force, (T-0).

3.5.2.1.4. By the acquiring organization in accordance with DoDFMR 7000.14-R, Volume 4, Chapter 6, *Property, Plant, and Equipment*, (T-0).

3.5.2.2. Established for capitalized IUS in the designated APSR, (T-0).

3.5.2.3. Established for IUS which does not meet the criteria for capitalization in the designated APSR or designated managerial system, (T-0).

3.5.2.4. Established for IUS in development in accordance with section 3.5.4., (T-0).

3.5.2.5. Enabled through unique identification (UID) standards, in accordance with DoDI 8320.03, *Unique Identification (UID) Standards for Supporting the DoD Information Enterprise*, (T-0).

3.5.2.6. Maintained by the accountable organization until formal relief of accountability through authorized means, such as transfer or disposal, (T-0).

3.5.3. **Accountable Records.**

3.5.3.1. The accountable organization will establish accountable records in the designated Accountable Property System of Record (APSR) for all capitalized Internal Use Software (IUS), (T-0).

3.5.3.1.1. A single record will be established for each IUS purchase or acquisition and all costs incorporated in accordance with the DoDFMR 7000.14-R, Volume 4, Chapter 6, *Property, Plant, and Equipment*, guidance, (T-0).

3.5.3.1.2. A single record will be established for each stand-alone COTS license with a unit cost that exceeds the capitalization threshold and is not a component of a developed system, (T-0).

3.5.3.1.3. A single record will be established for each distinct manufacturer part number on each purchase order for a bulk license purchase for COTS software, (T-0).

3.5.3.2. The accountable organization will maintain accountable records for non-capital IUS in the designated APSR or designated managerial system, (T-0).

3.5.3.3. The accountable organization will maintain accountable records for the life of the asset and will retain the records:

3.5.3.3.1. For 7 years after the end of the operational life of the developed IUS, (T-1).

3.5.3.3.2. For 7 years following the end of legal use for capitalized COTS, (T-1).
3.5.4. **Accountability of Software-in-Development.**

3.5.4.1. No formal property accountability (i.e., accountable property record) is established until Internal Use Software (IUS) development is completed, in accordance with section 3.5.2., (T-0).

3.5.4.2. Accountability is established in the APSR at the end of the development phase after the IUS developed has been final tested to verify that it meets specifications, (T-0).

3.5.4.2.1. The end of the development phase for major automated information systems will be the Full Deployment Decision (FDD), as described in DoDI 5000.02, *Operation of the Defense Acquisition System*, (T-0).

3.5.4.2.2. The end of the development phase for IUS that is not designated as major automated information systems will be the date that initial operating capability is established, (T-0).

3.5.4.2.3. IUS accountability also applies to National Security Systems, in accordance with DoDD 8000.01, *Management of the Department of Defense Information Enterprise (DoD IE)*, (T-0).

3.5.4.3. APSR records must be updated to reflect the physical changes made to the IUS and the associated costs when IUS enhancements, improvements, or other modifications occur, (T-0).

3.5.5. **Accountability of Commercial Internal Use Software (IUS) Licenses.**

3.5.5.1. Property accountability is required for commercial off-the-shelf (COTS) software licenses that meet all of the following criteria:

3.5.5.1.1. The COTS licenses are purchased for deployment to end user personal computing devices or computer servers, (T-0).

3.5.5.1.2. The COTS is purchased through a financial transaction or received as an IUS asset transfer from another entity, (T-0).

3.5.5.2. The IUS asset for a COTS license is the license agreement and record of ownership, such as the purchase order, contract, or assignment of licenses documentation for a transfer, (T-0).

3.5.5.3. The accountable organization will establish accountability for COTS IUS licenses:

3.5.5.3.1. Upon acceptance of the software order by the receiving organization for software licenses procured directly by the government, (T-0).

3.5.5.3.2. Upon the date the transfer occurs for commercial off-the-shelf (COTS) licenses received by the Air Force as an asset transfer from another entity, (T-0).

3.5.5.4. For bulk purchased software, units will record and track bulk license purchases as follows:, (T-0).

3.5.5.4.1. If the cost is below the capitalization threshold, the bulk license purchase should be expensed, (T-0).
3.5.5.4.2. For any purchase order or license transfer for which the total value of the COTS software licenses exceeds the capitalization threshold, the bulk license purchase should be capitalized, (T-0).

3.5.5.4.3. For COTS licenses procured through a bulk purchase and intended for use in or integration into developed Internal Use Software (IUS), the software licenses are accountable as part of the bulk license purchase and should not be allocated or otherwise associated with any developed IUS, (T-0).

3.5.5.5. COTS software licenses purchased for use in or integration with developed IUS will be included with the developed IUS, unless the licenses are procured through a bulk license purchase, in which case the provisions for bulk license purchases apply. Individual license accountability is not applicable, (T-0).

3.5.5.5.1. For bulk COTS software costs that will be capitalized, capitalized costs should include the amount paid to the vendor for the software and material internal costs incurred to implement the COTS software and otherwise make it ready for use. License maintenance, conversion costs, or upgrade purchases should be treated according to the DoDFMR 7000.14-R, Volume 4, Chapter 6, Property, Plant, and Equipment, and are typically expensed, (T-0).

3.5.5.6. Accountability for commercial off-the-shelf (COTS) licenses ceases when:

3.5.5.6.1. The final term expires and the license owner has complied with the publisher terms and conditions for terminating the license for term license agreements, (T-0).

3.5.5.6.2. A perpetual license is removed from inventory (e.g., uninstalled from computer(s) or upon the appropriate disposal of the hard drive(s) to which the software was installed) and when the disposal of the license is made in accordance with the license terms and the conditions for terminating, transferring, or otherwise retiring the license are completed, (T-0).

3.5.5.6.3. The accountable organization will ensure that documentary evidence is recorded and maintained in accordance with Air Force records management requirements, (T-0).

3.5.6. Accountability of Internal Use Software (IUS) Delivered As A Service.

3.5.6.1. Any license provided to Air Force users as a service (i.e. cloud computing, software as a service, or other “as a service” software subscriptions) will only be considered accountable IUS assets if an Air Force organization is designated as the licensee and the license owner retains the right to take control of the license independent of the hosting arrangement, (T-0).

3.5.6.2. Any license that is provided to AF users on an AF computer or on a computer owned by a third party and is not licensed to the AF will not be accountable as a DoD IUS asset, (T-0).

3.5.6.3. COTS IUS that is provided to the AF as a service that meets the requirement for accountability as an IUS asset, in accordance with section 3.5.1., will be accountable using the provisions for accountability for COTS licenses in section 3.5.5., (T-0).
3.5.7. **Internal Use Software (IUS) Inventory.**

3.5.7.1. All accountable organizations must maintain up-to-date inventory records of IUS for which they are accountable, (T-0).

3.5.7.2. In order to support maintenance of an up-to-date inventory of IUS and meet financial reporting requirements, accountable organizations must process all inventory changes (i.e., receipts of IUS, transfers between DoD Components, or disposition) within 7 calendar days or the end of the month in which the financial event occurs, whichever is sooner, (T-0).

3.5.7.3. The accountable organization must take an inventory of accountable Internal Use Software (IUS) no less than annually by fiscal year end to assess the accuracy of IUS asset records, update IUS asset records, assess any IUS property loss experienced, and provide the status of verified assets for fiduciary reporting purposes, (T-0).

3.5.7.4. A minimum 98 percent inventory accuracy rate will be achieved and maintained for capitalized IUS asset records, (T-0).

3.5.7.5. Any property loss discovered during the inventory should be reported and an inventory adjustment should be performed in accordance with record adjustment procedures, (T-0).

3.5.7.6. An annual “true-up” of licenses is sufficient for inventory validation of affected IUS licenses. The true-up may be utilized in place of the 98 percent accuracy rate with only those impacted, non-capital IUS assets, (T-0).

3.5.7.7. Accountable organizations will retain details of the result of their most current annual inventory, (T-0).

3.5.8. **Disposal.**

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

3.5.8.1.1. Before the accountable organization disposes of commercial IUS, legal counsel should review all IUS licenses for any limitations or potential liability, (T-0).

3.5.8.1.2. Accountable organizations must consult all relevant parties before any IUS disposition activity, (T-0).

3.5.8.2. The IUS disposal process involves turn-in to the Defense Logistics Agency Disposition Services and, in some cases, destruction, (T-0).

3.5.8.2.1. The disposal process should be executed in accordance with DoD Manual 4160.21, *Defense Materiel Disposition*, unless there is a conflict with the terms and conditions of the software license agreements or contracts, in which case the software license agreement and contract will take precedence, (T-0).

3.5.8.3. When Internal Use Software (IUS) is transferred, reassigned, exchanged, or sold to government or non-government organizations, the original documentation and media disks for the IUS must accompany it if the IUS was acquired commercially, (T-0).
3.5.8.3.1. In these instances, the original owner of the IUS must execute proper license transfer documentation with the manufacturer, (T-0).

3.5.8.4. Disposal is not complete unless all copies of the targeted IUS are uninstalled from the accountable organization’s network through uninstall procedures or proper disposition of the computer hardware or hard drive upon which the software is installed, (T-0).

3.5.8.5. The accountable organization will document the destruction, or vendor return, of IUS and report it to an adjunct APO. This will include a statement verifying that all media, licenses, and documentation have been destroyed or returned to the vendor, (T-0).

3.5.9. Valuation.

3.5.9.1. Valuation is required for Capital Internal Use Software (IUS), (T-0).

3.5.9.1.1. All IUS will be capitalized when meeting the following criteria:

   3.5.9.1.1.1. Total acquisition cost is greater than or equal to $250,000, (T-0).

   3.5.9.1.2. Useful life of the IUS is greater than or equal to 2 years, (T-0).

3.5.9.2. IUS will be capitalized at full cost, which is comprised of the acquisition cost and other associated costs as outlined in Table 3.1., (T-0).

Table 3.1. Internal Use Software (IUS) Capitalization Cost Determination.

<table>
<thead>
<tr>
<th>Project Phase</th>
<th>Task</th>
<th>Treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preliminary Design:</td>
<td>Project Evaluation or Need Determination</td>
<td>Expense</td>
</tr>
<tr>
<td>Conceptual Planning/Planning &amp; Requirements</td>
<td>Concept Formulation and Testing</td>
<td>Expense</td>
</tr>
<tr>
<td></td>
<td>Evaluation and Testing of Alternatives</td>
<td>Expense</td>
</tr>
<tr>
<td></td>
<td>Project Approval</td>
<td>Expense</td>
</tr>
<tr>
<td>Software Development:</td>
<td>Design, Including Software Configuration and Software Interfaces</td>
<td>Capitalize</td>
</tr>
<tr>
<td>Design/Development &amp; Testing/Implementation</td>
<td>Coding</td>
<td>Capitalize</td>
</tr>
<tr>
<td></td>
<td>Installation to Hardware</td>
<td>Capitalize</td>
</tr>
<tr>
<td></td>
<td>Project Personnel Costs</td>
<td>Capitalize</td>
</tr>
<tr>
<td></td>
<td>Testing, Including Parallel Processing</td>
<td>Capitalize</td>
</tr>
<tr>
<td></td>
<td>Quality Assurance Testing</td>
<td>Capitalize</td>
</tr>
<tr>
<td></td>
<td>Technical Documentation, Including User Manuals</td>
<td>Capitalize</td>
</tr>
<tr>
<td></td>
<td>Data Conversion Software</td>
<td>Expense</td>
</tr>
<tr>
<td></td>
<td>General and Admin Costs</td>
<td>Expense</td>
</tr>
</tbody>
</table>
### Operational Software:
Operations & Maintenance / Disposition

<table>
<thead>
<tr>
<th>Enhancements</th>
<th>Capitalization Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training</td>
<td>Expense</td>
</tr>
<tr>
<td>Data Conversion, Includes Cleansing, Deleting, and Repackaging of Data</td>
<td>Expense</td>
</tr>
<tr>
<td>Help desk</td>
<td>Expense</td>
</tr>
<tr>
<td>Application Maintenance/Bug Fix</td>
<td>Expense</td>
</tr>
</tbody>
</table>

3.5.9.3. When acquisition cost is unknown, reasonable estimates of the historical acquisition cost may be used, (T-0).

3.5.10. Additional Resources. For additional detail on IUS Accountability, refer to DoDI 5000.76, *Accountability and Management of Internal Use Software (IUS)*.

BRADFORD J. SHWEDO, Lt Gen, USAF  
Chief, Information Dominance and  
Chief Information Officer
Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Executive Order 13103, Computer Software Piracy, 30 September 1998
Executive Order 13589, Promoting Efficient Spending, 9 November 2011
The Copyright Act of 1976
FAR, Subpart 7.5, Inherently Governmental Functions, FAC 2005-97, 13 January 2017
DFARS, Subpart 217.70, Exchange of Personal Property, 28 December 2017
DoDFMR, 7000.14-R, Vol 1, Chapter 9, Financial Records Retention, February 2016
DoDFMR 7000.14-R, Volume 3, Chapter 8, Standards for Recording and Reviewing Commitments and Obligations, February 2016
DoDFMR 7000.14-R, Volume 4, Chapter 6, Property, Plant, and Equipment, June 2009
DoDD 8000.01, Management of the Department of Defense Information Enterprise (DoD IE), 17 March 2016
DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 14 April 2004
DoDI 4151.19, Serialized Item Management (SIM) for Life-Cycle Management of Materiel, 9 January 2014
DoDI 5000.02, Operation of the Defense Acquisition System, 7 January 2015
DoDI 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property, 27 April 2017
DoDI 5000.76, Accountability and Management of Internal Use Software (IUS), 2 March 2017
DoDI 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI), 21 April 2016
DoDI 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense, 5 August 2013
DoDI 8320.03, Unique Identification (UID) Standards for Supporting the DoD Information Enterprise, 4 November 2015
DoDI 8330.01, Interoperability of Information Technology (IT) Including National Security Systems (NSS), 21 May 2014
DoDI 8500.01, Cybersecurity, 14 March 2014
DoD Manual 4160.21, Defense Materiel Disposition, 22 October 2015
DoDM 5400.-7-R_AFMAN33-302, Freedom of Information Act Program, 21 October 2010
ISO/IEC 19770, Software Asset Management (SAM)
ISO/IEC 20000, Information Technology - Service Management
AFPD 10-6, Capabilities Requirements Development, 6 November 2013
AFPD 17-1, Information Dominance Governance and Management, 12 April 2016
AFPD 17-2, Cyberspace Operations, 12 April 2016
AFI 16-201, Air Force Foreign Disclosure and Technology Transfer Program, 2 June 2015
AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT), 2 February 2017
AFI 17-130, Cybersecurity Program Management, 31 August 2015
AFI 17-210, Radio Management, 26 May 2016
AFI 21-103, Equipment Inventory, Status and Utilization Reporting, 16 December 2016
AFI 23-119, Exchange, Sale, or Temporary Custody of Non-excess Personal Property, 5 June 2001
AFI 65-201, Managers’ Internal Control Program Procedures, 9 February 2016
AFMAN 17-1301, Computer Security (COMPUSEC), 10 February 2017
AFMAN 23-220, Reports of Survey for Air Force Property, 1 July 1996
AFMAN 33-363, Management of Records, 1 March 2008

Prescribed Forms
No forms are prescribed by this publication

Adopted Forms
DD Form 200, Financial Liability Investigation of Property Loss
DD Form 250, Material Inspection and Receiving Report
DD Form 1149, Requisition and Invoice/Shipping Document
DD Form 1348-1A, Issue Release/Receipt Document
AF Form 847, Recommendation for Change of Publication
AF Form 2519, All Purpose Checklist
**Abbreviations and Acronyms**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AF</td>
<td>Air Force</td>
</tr>
<tr>
<td>AFECO</td>
<td>Air Force Equipment Control Officer</td>
</tr>
<tr>
<td>AFEMS</td>
<td>Air Force Equipment Management System</td>
</tr>
<tr>
<td>AFI</td>
<td>Air Force Instruction</td>
</tr>
<tr>
<td>AFMAN</td>
<td>Air Force Manual</td>
</tr>
<tr>
<td>AFMC</td>
<td>Air Force Materiel Command</td>
</tr>
<tr>
<td>AFPD</td>
<td>Air Force Policy Directive</td>
</tr>
<tr>
<td>AFPSC</td>
<td>Air Force Space Command</td>
</tr>
<tr>
<td>AFWay</td>
<td>Air Force Way</td>
</tr>
<tr>
<td>AIM</td>
<td>Asset Inventory Management</td>
</tr>
<tr>
<td>APSR</td>
<td>Accountable Property System of Record</td>
</tr>
<tr>
<td>BSLM</td>
<td>Base Software License Manager</td>
</tr>
<tr>
<td>C4</td>
<td>Command, Control, Communications, and Computers</td>
</tr>
<tr>
<td>CAGE</td>
<td>Commercial and Government Entity code</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off-the-Shelf</td>
</tr>
<tr>
<td>CS</td>
<td>Communications Squadron</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DoDD</td>
<td>Department of Defense Directive</td>
</tr>
<tr>
<td>DoDFMR</td>
<td>Department of Defense Financial Management Regulation</td>
</tr>
<tr>
<td>DoDI</td>
<td>Department of Defense Instruction</td>
</tr>
<tr>
<td>DRU</td>
<td>Direct Reporting Unit</td>
</tr>
<tr>
<td>ECO</td>
<td>Equipment Control Officer</td>
</tr>
<tr>
<td>ELA</td>
<td>Enterprise License Agreement</td>
</tr>
<tr>
<td>E.O</td>
<td>Executive Order</td>
</tr>
<tr>
<td>ESI</td>
<td>Enterprise Software Initiative</td>
</tr>
<tr>
<td>FAR</td>
<td>Federal Acquisition Regulation</td>
</tr>
<tr>
<td>FOA</td>
<td>Field Operating Agency</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITAM</td>
<td>Information Technology (IT) Asset Management</td>
</tr>
<tr>
<td>IUS</td>
<td>Internal Use Software</td>
</tr>
</tbody>
</table>
MAJCOM—Major Command
MECO—Major Command Equipment Control Officer
MOA—Memorandum of Agreement
OPR—Office of Primary Responsibility
PWCS—Personal Wireless Communications Systems
SAF—Secretary of the Air Force
SPI—Software Process Improvement

Terms
Acceptance — A formal certification that the goods or services have been received and that they conform to the terms of the contract. See Federal Acquisition Regulation Part 46 for contractual requirements and procedures that constitute acceptance.

Accountability — The obligation imposed by law, lawful order, or regulation, accepted by an organization or person for keeping accurate records and to ensure control of property, documents or funds, with or without physical possession. The obligation, in this context, refers to the fiduciary duties, responsibilities, and obligations necessary for protecting the public interest; however, it does not necessarily impose personal liability upon an organization or person.

Accountable Officer — An individual appointed by proper authority who maintains items and/or financial records in connection with government property, irrespective of whether the property is in his or her possession for use or storage, or is in the possession of others to whom it has been officially entrusted for use or care and safekeeping. In all cases, the accountable officer is responsible for establishing and maintaining financial property control records, controlling the processing of supporting documentation, and maintaining supporting document files. The primary accountable officers under the Air Force ROS System include: chief of supply, medical supply officer, munitions officer, fuels officer, communications and information systems officer, civil engineer, etc.

Accountable Property Officer (APO) — An individual who, based on his or her training, knowledge, and experience in property management, accountability, and control procedures, is appointed in writing through the DoD Component procedures to establish and maintain an organization’s accountable property records, systems, or financial records, in connection with government property, irrespective of whether the property is in the individual’s possession.

Accountable Property Record — The record contained within the APSR.

Accountable Property System of Record (APSR) — The government system used to control and manage accountable property records. A subset of existing organizational processes related to the lifecycle management of property; the system that is integrated with the core financial system. The APSR may also control and manage accountability records as described in Paragraph 2.1.

Accountability Record — A record maintained for managerial rather than financial reporting purposes. Accountability records should be used when the property does not meet the accountable property record requirements (Paragraph 2.1) but does require active management based on other than financial criteria.
Acquisition — Acquiring hardware, supplies, or services: Through purchase, lease, or other means, including transfer or fabrication, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated; or by contract with appropriated funds of supplies or services.

Acquisition Cost — The amount, net of both trade and cash discounts, paid for the property, plus transportation costs and other ancillary costs. See “full cost.”

Automated Inventory Tool (AIT) — The family of technologies that improves the accuracy, efficiency, and timeliness of material identification and data collection. AIT media and devices include, but are not limited to, linear and two-dimensional bar code symbols and their readers; magnetic stripe cards; integrated cards, (i.e., smart cards; optical memory cards); radio frequency identification (active and passive); contact memory-button devices; and magnetic storage media.

Capital Asset — An asset that meets or exceeds the capitalization threshold found in DoDFMR 7000.14-R, Volume 4, Chapter 6, Property, Plant, and Equipment, for the DoD Component.

Capital Lease — Leases that transfer substantially all the benefits and risks of ownership to the lessee. If at its inception, a lease meets one or more of the following criteria, the lease is considered a capital lease: 1) the lease transfers ownership of the property to the lessee by the end of the lease term, 2) the lease contains an option to purchase the leased property at a bargain price, 3) the lease term (non-cancelable portion, plus all periods, if any, representing renewals or extensions that can reasonably be expected to be taken) is equal to or greater than 75 percent of the estimated economic life of the leased property, and 4) the present value of rental and other minimum lease payments, excluding that portion of the payments representing executory cost, equals or exceeds 90 percent of the fair value of the leased property. See DoDFMR 7000.14-R, Volume 4, Chapter 6, Property, Plant, and Equipment, for procedures and additional information.

Command, Control, Communications, and Computer (C4) Systems — Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander’s exercise of command and control, across the range of military operations. Also called “communications and information systems.”

Commercial Off-the-Shelf (COTS) Software — Software developed, tested, and sold by commercial companies to the general public. This software meets operational requirements without modification or alteration to perform on a DOD network or computer. Examples include word processors, databases, application generation, drawing, compiler, graphics, communications, and training software.

Computer System — A functional unit, consisting of one or more computers and associated software, that (1) uses common storage for all or part of a program and also for all or part of the data necessary for the execution of the program; (2) executes user-written or user-designated programs; and (3) performs user-designated data manipulation, including arithmetic and logic operations. Note: A computer system is a stand-alone system or may consist of several interconnected systems. Personal computers, microcomputers, minicomputers, multi-user systems, all standard multi-user small computer requirements contract systems, text processors, word processors, intelligent typewriters, and workstations are examples of computer systems.

Contract — Any enforceable agreement, including rental and lease agreements and purchase orders, between an agency and a business concern for the acquisition of property or services.
Documentation — Records required to plan, develop, operate, maintain, and use electronic records and software. Included are systems specifications, file specifications, code books, record layouts, user guides, and output specifications.

End User Devices — Desktops, notebooks, tablets, accessories, mobile devices (e.g., blackberry, smart phones, pagers), phones (e.g., desk phones), that are used by end users.

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

Equipment — Personal property that is functionally complete for its intended purpose, durable, and nonexpendable. Equipment generally has an expected service life of two years or more; is not intended for sale; does not ordinarily lose its identity or become a component part of another article when put into use; has been acquired or constructed with the intention of being used.

Equipment Control Officer (ECO) — An individual appointed by the applicable Host/Tenant APO to manage and control Information Technology (IT) assets for an installation.

Found—on-Base (FOB) - Any IT hardware equipment found in the Unit APO-owned area that is not on the current inventory listing.

Full cost — A baseline value that includes all material costs incurred to acquire and bring the property to a form and location suitable for its intended use and, as applicable, depreciated over its useful life.

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

Host APO — Accountable property officer appointed by the Installation Commander to manage the Information Technology Asset Management (ITAM) program for the Installation.

Information Technology (IT) — Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the DoD component. For the purposes of the preceding sentence, equipment is used by a DoD component if the equipment is used directly or is used by a contractor under a contract with the DoD component that (1) requires the use of such equipment; or (2), requires the use to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term Information Technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services) and related resources. Notwithstanding the above, the term information technology does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract (DoDD 8000.01, Management of the Department of Defense Information Enterprise (DoD IE)).
Key Supporting Documents — Documentation needed by transaction type to support the relevant financial statement assertion. Examples include purchase invoices, contracts, DD Forms 1149, 1348-1A, 200, etc.

License Agreements — Contracts between the software publisher and the user that instructs and limits the software use. When purchasing software, the buyer only acquires a license to use it. The publisher retains the full rights to the software and has the sole right to its further distribution and reproduction.

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

Maintenance — (1) All action taken to retain materiel in or to restore it to a specified condition. It includes: inspection, testing, servicing, classification as to serviceability, repair, rebuilding, and reclamation. (2) All supply and repair action taken to keep a force in condition to carry out its mission. (3) The routine recurring work required to keep a facility (plant, building, structure, ground facility, utility system, or other real property) in such condition that it is continuously utilized, at its original or designed capacity and efficiency, for its intended purpose. (4) The function of keeping C4 items of equipment in, or restoring them to, serviceable condition. Maintenance is not intended to increase the value, capabilities, or expected life of a system. Equipment maintenance includes servicing, repair, modification, modernization, overhaul, inspection, condition determination, corrosion control, and initial provisioning of support items. Maintenance includes both preventive and corrective actions. Software maintenance includes anticipating, detecting, and eliminating errors.

Major Command Equipment Control Officer (MECO) — The individual appointed by the MAJCOM, FOA, and DRU, or equivalent that oversees the management and control of IT assets within their area of responsibility.

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

Personally Identifiable Information — Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother’s maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Physical Inventory— The verification of property existence, accountable property record completion, location, and quantity. The process may also involve verifying additional information, performing reconciliations, and modifying the accountable property records. Also see ASTM International E-2135-10ae1 for voluntary consensus standards on conducting a physical inventory.

Pilferable Items — Property that has a ready resale value or application to personal possession, and that are therefore especially subject to theft.
Property — Equipment, weapon systems, and other accountable property (e.g., administrative property, special tools, special test equipment). Other types of personal property, such as supplies, material, and records, are not included in this definition unless expressly stated as being included.

Receipt — A transmission or other acknowledgment made by a receiving entity to indicate that a message, good, or service has been satisfactorily received. Receipt is often denoted by signing a situation specific form, such as DD Forms 250, 1149, “Requisition and Invoice/Shipping Document,” or 1348-1A, “Issue Release/Receipt Document.”

Reconciliation — The process of aligning the physical count with the quantity posted to the accountable property records, researching discrepancies, and determining inventory accuracy, i.e., calculation of loss or overage rates.

Requirement — A need for a new or improved information processing capability that, when satisfied, increases the probability of operational mission success or decreases the cost of mission support.

Reuse — The process of developing or supporting a software-intensive system using existing software assets.

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

System — A set of IT components and their external peripherals and software interconnected with another set. Typical systems include notebook computers, desktop PCs, networked and distributed systems (e.g., servers, workstations, data management processors, etc.), mainframe and midsize computers and associated peripherals.

Tenant APO — Accountable property officer of a tenant organization for which the installation does not support Information Technology Asset Management (ITAM) for the tenant organization as stipulated in the Host Tenant Support Agreement.

Unit APO — The commander of an organization which has custodial responsibility for information technology assets.
Attachment 2

DESIGNATED ACCOUNTABLE PROPERTY SYSTEM OF RECORD (APSR) GUIDANCE

A2.1. Purpose and Scope. This attachment provides guidance for use of the designated APSR. SAF/CIO A6 has designated AFEMS-AIM as the Accountable Property System of Record for Information Technology (IT) hardware assets. The Air Force Medical Operations Agency (AFMOA) has designated the Defense Medical Logistics Standard Support (DMLSS) system as the medical War Reserve Material (WRM) IT hardware asset accountability system.

A2.2. AFEMS-AIM Roles and Responsibilities.

A2.2.1. Primary and Alternate Major Command Equipment Control Officer (MECO).

A2.2.1.1. Provides guidance and procedural policy to the ECOs regarding management of IT/Personal Wireless Communications Systems (PWCS) assets.

A2.2.1.2. Approves or rejects transfer of IT/PWCS assets between losing and gaining commands, (T-1).

A2.2.1.3. Reviews finalized excess reports completed by applicable ECOs and ensures appropriate action is accomplished.

A2.2.1.4. Coordinates on the establishment of a new Primary Asset Account and the IT/PWCS data system connectivity, as required.

A2.2.1.5. Manages the IT/PWCS Primary ECO user roles.

A2.2.1.6. Establishes accountability for IT/PWCS assets acquired through joint services PMs, as required.

A2.3.1. Primary and Alternate Equipment Control Officer (ECO).

A2.3.1.1. Loads all Information Technology (IT) and Personal Wireless Communications Systems (PWCS) asset records, (T-1).

A2.3.1.2. Ensures correct MAJCOM code is entered into AFEMS-AIM for all IT/PWCS assets in their respective DRA. Ensures the IT/PWCS asset status code(s) in AFEMS-AIM is updated as required.

A2.3.1.3. Reviews the IT asset status codes periodically to ensure the codes reflect the current status.

A2.3.1.4. Creates all new accounts within their DRA and modifies the applicable Primary and Alternate Equipment Custodians (EC), (T-1).

A2.3.1.5. Processes receipt, transfer, and disposition of Information Technology (IT) assets in AFEMS-AIM, (T-1).

A2.3.1.6. Assists the EC in determining the ownership of all Found on Base (FOB) assets, (T-2).

A2.3.1.7. Directs Unit APOs to conduct complete inventories of all assets assigned to the Unit APO (ECOs have the authority to lock Unit APO accounts until the inventories are completed), (T-1).
A2.3.1.8. Ensures all assets are labeled with CAGE Code, Part Number, and Serial Number, (T-1).

A2.3.1.8.1. If manufacturer labels do not contain proper identification, produces AFEMS-AIM-generated standard product (bar code) labels for the Unit APO, (T-1).

A2.3.1.8.2. If AFEMS-AIM-generated standard product labels cannot be produced, establishes local labels that contain proper identification and provide them to the Unit APO, (T-1).

A2.3.1.9. Adjusts inventories once loss/gain discrepancies have been reconciled, (T-2).

A2.3.1.10. Codes deployable IT/PWCS assets in the AFEMS-AIM database, (T-1).

A2.3.1.11. Prepares the necessary shipping documents for items that are excess and required by other services, (T-3).

A2.4.1. **Auditor - Requires AFECO approval.**

A2.4.1.1. Provides the capability to view AFEMS-AIM data and to produce Discoverer reports.

A2.5.1. **AFEMS-AIM User Guide.** For specific instructions on how to perform AFEMS-AIM functions, utilize the AFEMS-AIM User Guide link located on the AFECO Collaboration Site.
Attachment 3

INFORMATION TECHNOLOGY (IT) HARDWARE ENTERPRISE INVENTORY PLAN

A3.1. Purpose and Scope. The intent of this plan is to articulate the minimum requirements for performing asset/item inventories for IT hardware assets. Additional requirements that may be levied onto units by their parent MAJCOM/DRU/FOA organization will be articulated in a MAJCOM/DRU/FOA-specific Inventory Plan.

A3.2. Inventory Frequency.
A3.2.1. Assets meeting the criteria stated in paragraph 2.1.1.1. will be inventoried annually.
A3.2.2. Assets meeting the criteria stated in paragraph 2.1.1.2. will be inventoried every three years.

A3.3. Preparing for Inventory.
A3.3.1. To prepare for an asset inventory, a baseline of the asset account will be produced by the ECO and provided to the Unit APO.
A3.3.2. To assist in this process, the account owner can use a combination of asset discovery/automated inventory tools and manual identification of assets.
A3.3.2.1. The account owner can utilize enterprise asset discovery tools to perform a network scan to “discover” assets on the network that are within their account.
A3.3.3. This discovery cannot be done any earlier than one month prior to the inventory due date.
A3.3.4. One month of scanning will produce a list of assets that have been on the network at various times over that scanning period and this list can be included as a component of the inventory of a complete account.

A3.4. Performing the Inventory. To perform an asset inventory, the Unit APO:
A3.4.1. Will ensure that all assets in their account(s) have been identified.
A3.4.2. Will ensure that gains/losses against the inventory baseline are documented and reconciled.
A3.4.3. If using Automated Inventory Tool (AIT), the physical inventory can be performed only on those assets not identified using the AIT.

A3.5. Completing the Inventory. To complete an asset inventory, the Unit APO:
A3.5.1. Will ensure that the individual performing the inventory has signed, indicating that the inventory is complete and accurate.
A3.5.2. Will endorse the signed inventory with signature, accepting responsibility for the results.
A3.5.3. Will provide the completed, signed, and endorsed inventory in an electronic format to the installation ECO for record.
A3.6. **Finalizing the Inventory.** To finalize an asset inventory, the ECO will reconcile all gain/loss annotations in the designated Accountable Property System of Record (APSR).

A3.7. **Random Sampling.** Random sampling of the Information Technology (IT) asset enterprise will be performed by the AFECO to ensure that inventory requirements are being adhered to.