BY ORDER OF THE COMMANDER
TINKER AIR FORCE BASE

TINKER AIR FORCE BASE
INSTRUCTION 17-1203

6 AUGUST 2025

Cyberspace

INFORMATION TECHNOLOGY (IT)
ASSET MANAGEMENT (ITAM)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: 72ABW/SCXO

Certified by: 72ABW/SC
(Michael C. Wiles)

Supersedes: TINKERAFBI17-1203, 12 September 2024

Pages: 17

This instruction implements DAFMAN 17-1203, *Information Technology Asset Management (ITAM)*. This instruction establishes local procedures for the procurement, management, and protection of Information Technology (IT) hardware assets and IT software assets. **Note:** DAFMAN 17-1203 will be referenced for primary IT Asset Management (ITAM) requirements. This instruction applies to all AFMC unit and host tenant units attached to the Air Force Network (AFNet) and includes standalone systems of Air Force organizations at Tinker Air Force Base (AFB). Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AFI 33-322, *Management of Records,* and disposed of in accordance with (IAW) Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional point of contact's chain of command. This publication may not be supplemented or further implemented/extended.

SUMMARY OF CHANGES

This instruction has been revised to supersede TAFBI33-112, *Information Technology Hardware Asset Management*, 21 June 2016 and TAFBI33-534, *Software Management*, 25 April 2017. This instruction is now formatted to reflect changes implemented in DAFMAN 17-1203, *Information Technology Asset Management, 13 Sep 2022*. This instruction should be reviewed in its entirety.

Chapter 1

OVERVIEW

1.1. Overview. It is the responsibility of each individual who procures, manages, and/or uses government IT hardware and software assets to ensure strict accountability is maintained of those assets. Both physical and informational security will be maintained on each accountable government asset from the time of procurement until the time of disposal.

1.2. Roles and Responsibilities.

1.2.1. Equipment Control Officer (ECO): The ECO maintains ultimate responsibility for the management of IT hardware assets within AFMC units and designated tenant units, as directed by the current Host Tenant Support Agreement, at Tinker Air Force Base. The ECO will:

1.2.1.1. Coordinate all unit ITAM inventory management issues through the unit Accountable Property Officer (APO) and, if applicable, Organization Computer Manager (OCM).

1.2.1.2. Inform Unit APOs and personnel of changes to ITAM regulation and maintain current training materials.

1.2.1.3. Conduct Staff Assist Visits (SAV) to ensure accountability and asset management processes are effective. SAV findings will be provided to the responsible unit APO when requested.

1.2.1.4. Utilize electronic methods to maintain all official records created as a result of ITAM Office practices in accordance with AFI 33-322.

1.2.1.5. Coordinate appropriate signatures on the transfer documents for any accountable IT assets transferring to a new installation. The gaining ECO and IT Property Custodian (PC) will be provided a copy of the completed transfer paperwork to be maintained as an official Key Supporting Document (KSD).

1.2.1.6. Provide initial and refresher ITAM training to PCs and OCMs. Maintain a current listing of all appointed PCs and OCMs.

1.2.1.7. Coordinate with PCs to assist organizations with the completion of Management Internal Control Toolset (MICT) requirements.

1.2.1.8. Inform PC of requirement to complete one for one asset swap(s) within 30 calendar days of receiving replacement assets.

1.2.1.8.1. Schedule PC disposition appointment at the time of replacement asset pickup.

1.2.2. Base Software License Manager (BSLM) responsibilities.

1.2.2.1. Provide software license training for newly appointed BSLM, Unit Software License Manager (USLM), and Client System Technicians (CST).

1.2.2.2. Ensure each unit maintains a software inventory of all government owned Internal Use Software (IUS), Commercial off-the-shelf (COTS), and freeware software in use.

1.2.2.3. Ensure each unit performs an annual inventory of all IUS, COTS, and/or freeware software licenses, and corresponding documentation of unit software. Ensure unit APO endorses inventory letter supplied to BSLM.

1.2.2.4. Maintain a current list of all appointed USLMs.

1.2.2.5. Ensure SCORE or current automated inventory tools, are used for tracking software installed on base network.

1.2.2.6. Ensure all software purchases follow the "General Guidelines for Acquisition of Software" as listed in DAFMAN 17-1203.

1.2.3. Unit Accountable Property Officers (APOs): Commanders (or their equivalent) are responsible for providing guidance 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:

1.2.3.1. Accept responsibility for the accountability of all IT hardware and software assets assigned to their unit.

1.2.3.2. Designate custodial areas within an accountable area that can be physically inventoried within two (2) workdays or less and should not span multiple buildings. It is suggested, PCs be physically located near their designated custodial area. Each designated custodial area will be managed using the SAF/CIO A6 designated Accountable Property System of Record (APSR).

1.2.3.3. Appoint, at minimum, one primary and one alternate PC for each designated custodial areas.

1.2.3.3.1. Replacement PC no later than 45 calendar days prior to the projected departure of the current PC.

1.2.3.3.2. Replace PC that will be deployed, assigned temporary duty (TDY), or unable to perform PC duties for more than 179 DAYS.

1.2.3.3.3. Ensure complete out-processing for departing PC upon transfer of account. This requires assignment of a new PC and a completed joint loss-gain inventory of IT assets when the Primary PC is being replaced.

1.2.3.4. Approve PC be relieved of other responsibilities during mandatory annual inventories until such time as the inventory has been completed.

1.2.3.5. Ensure positive action is taken to properly account for and secure excess IT equipment during unit moves, reorganizations, or facility remodeling.

1.2.3.6. Email the ECO, at **72abw.scxo.itam.work@us.af.mil**, to authorize the transfer of excess or re-obligated IT assets to a new Accountable Unit Identification Code (AUIC).

1.2.3.7. Adhere to the Financial Liability Investigation (FLI) timeframes and guidance outlined in DoD 7000.14-R, Financial Management Regulation, Volume 12, Chapter 7 *Financial Liability For Government Property* for any lost, stolen, or damaged IT assets requiring an investigation.

1.2.3.8. Determine a threshold of acceptable risk for pilferable and non-accountable IT assets still requiring management to ensure reasonable insulation from theft. IT assets not meeting the accountable property threshold as defined in DAFMAN 17-1203, monitors, Voice over Internet Protocol (VOIP) phones, mice, etc.

1.2.3.8.1. Document a definition of IT assets to be managed as pilferable and provide to their organization's Government Purchase Card (GPC) holder. For example, a stated threshold could be "any asset with a purchase price of $400 or more." Unit APOs or their designated delegates will ensure IT assets meeting the stated criteria are tracked and made available to the GPC holder for audit purposes.

1.2.3.8.2. Ensure construction of an automated tracking system IAW DoDI 5000.64 to track assets meeting the organization's pilferable asset definition. **Figure A2.1** may be used as a template to create a pilferable or non-accountable tracking spreadsheet.

1.2.3.9. Annually designate custodial responsibilities within accountable areas and appoint, at minimum, a primary and alternate USLM to the BSLM in support of the Software License Management Program. USLM appointment letter will be IAW guidelines established by the BSLM.

1.2.3.9.1. Annual appointment must be completed NLT 365 calendar days from the date the Unit APO signed the current appointment letter.

1.2.3.9.2. Appoint replacement USLMs NLT 45 calendar days prior to the projected departure of the current USLM.

1.2.3.9.3. If a USLM will be deployed, TDY, or unable to perform SLM duties for more than 179 days he/she must be replaced on the applicable USLM account.

1.2.3.10. Ensure custodial areas are wisely designated for a manageable span of control for USLMs. Custodial areas can be consolidated to allow accountabilities for all units under span of control for Unit APO's.

1.2.3.11. Annually certify and document the account has completed all annual requirements. This certification is documented by signing an annual memorandum indicating the account has completed all requirements no later than 365 days from the last account certification and submitting it to the BSLM. Annual requirements can be found in **para 1.2.6.1** of this instruction. Failure to provide BSLM with annual requirements may cause the account to be locked with restrictions as described in **para 3.1.2** of this publication and sub-sections.

1.2.3.12. Ensure software acquisitions are submitted and approved IAW current 72d Communications Directorate Guidance.

1.2.4. Organization Computer Manager (OCM): An OCM may be appointed by the Unit APO/Commander as the focal point for computer operation issues. The OCM will:

1.2.4.1. Submit an OCM appointment letter identifying each ITAM account under his/her management. The OCM appointment letter will be resubmitted as changes occur. The OCM appointment letter format will be IAW guidelines established by the ECO.

1.2.4.2. Complete initial PC training or have been an PC within the past calendar year.

1.2.4.3. Validate ITAM requirements within their organization.

1.2.4.4. Advise/assist PC in accomplishing their assigned duties and responsibilities IAW with direction from the ECO.

1.2.4.5. Coordinate with the ECO and PC to ensure completion of all annual requirement packages.

1.2.5. Property Custodian (PC): Manage IT assets within their area of responsibility and are accountable to the ECO for all IT assets on their inventory. PC will:

1.2.5.1. Initially receive formal classroom or other approved training conducted by the ECO prior to accepting responsibility for an ITAM account. The ECO schedules the class size and frequency of this training.

1.2.5.2. Initial training certificates will be valid for three months after training is completed.

1.2.5.3. If not added to an ITAM account within three (3) months, refresher training will be completed before an PC can be added to the requested account.

1.2.5.4. Re-accomplish ITAM Training NLT 365 calendar days from the date training was last completed. This requirement will be fulfilled using a training link provided on the Tinker ITAM SharePoint site.

1.2.5.5. Coordinate with the ECO and OCM regarding all ITAM inventory management issues. This includes change of assigned PC or change of ITAM account status.

1.2.5.6. Maintain organized and official records of all actions performed on their ITAM account(s) IAW AFI 33-322 and the ECO.

1.2.5.7. Account for all IT assets according to Serialized Item Management (SIM) and Item Unique Identification (IUID) guidance in *AFI 63-101/20-101, Integrated Life Cycle Management.*

1.2.5.8. Route requests for annual inventory suspense extensions to the ECO through the Unit APO. Extensions are approved in two-week intervals. Requests not routed through the Unit APO may be disapproved.

1.2.5.9. Ensure appropriate APSR generated, IUID or equivalent labels are located on each IT asset listed on their inventory. Labels must be accurate, legible, and current at all times. New labels are required when a label is no longer legible, incorrect, or not present. Labels are available upon request from the ECO.

1.2.5.10. Coordinate with the ECO to add newly acquired accountable IT hardware to their account when it becomes government property. The information required to add new equipment to the designated APSR must be provided to the ECO within five (5) business days of delivery. Requests to add equipment to the designated APSR will be submitted using Tinker Form 30, *Accountable Asset Add or Government Purchase Card (GPC)*. The form is available on the Tinker ITAM SharePoint site.

1.2.5.11. Coordinate with ECO to transfer accountable IT hardware assets between accounts within the same UIC. Transfer requests will be submitted using Tinker Form 32, *Computer System Equipment Action*. The form is available on the Tinker ITAM SharePoint site.

1.2.5.12. Review their ITAM account(s) every 365 days for excess IT assets. It is recommended, IT assets deemed excess and in good working condition are posted on the ITAM Office's "Available Excess IT Asset Listing" for re-utilization on Tinker AFB.

1.2.5.13. Notify the ECO using the Tinker Form 32; prior to deploying, shipping, or transferring of accountable IT assets outside of Tinker AFB.

1.2.5.14. Coordinate with the ECO to complete one for one asset swaps within 30 calendar days of receiving replacement assets.

1.2.5.15. Ensure all batteries and hard drives are removed from IT equipment being turned-in for disposition.

1.2.5.15.1. If units do not have adequate space, storage, or equipment to complete removal before turn-in, the Disposition Office will provide necessary equipment, space, and training to complete removal of batteries and hard drives during disposition appointments.

1.2.6. Unit Software License Manager (USLM): Manage software licenses/assets within their area of responsibility and are accountable to the BSLM for all software licenses/assets on their inventory. USLMs will:

1.2.6.1. Annually perform the software asset management duties listed below for their appointed units.

1.2.6.2. Inventory of the custodial areas installed/owned software. Failure to provide BSLM with annual requirements may cause the account to be locked with restrictions as described in **para 3.1.2** of this instruction and sub-sections.

1.2.6.3. Update USLM training annually through the BSLM.

1.2.6.4. Coordinate with the BSLM, functional system administrators, CSTs, and software purchasers when new software is being purchased.

1.2.6.5. Monitor delivery of all new software and update software folders in a timely manner IAW DAFMAN 17-1203.

1.2.6.5.1. Store evidence of license agreements or licenses (e.g., user manuals, purchase documentation, CD-ROMs, etc.) and physical software media in a secure centralized location (e.g., locked drawer, file cabinet, room, etc.). Work with local Records Inventory Manager or Base Records Management Office to ensure proper retention and disposition of official records and records approval in the office file system.

1.2.6.5.2. Use BSLM provided account folders in SharePoint to load corresponding account records as listed below.

1.2.6.5.3. Maintain a hard or soft copy of the software license inventory.

1.2.6.5.4. "Proof-of-License Ownership" of all COTS/IUS in use within their custodial area. Proof may consist of hardcopy or softcopy documentation from the supplier such as manual, purchase documentation, email, or distribution media.

1.2.6.5.5. Purchase requests associated with license purchases by the current 72 ABW/SC directed process.

1.2.6.6. Ensure the legal use of all software for the unit IAW the End-User License Agreement (EULA).

1.2.6.6.1. Each COTS application must have a license.

1.2.6.6.2. Use of software corresponds to the applicable license agreement.

1.2.6.6.3. Freeware software, when applicable by EULA, has a purchased license and is listed as approved for the Base network.

1.2.6.7. Request approval for disposal/redistribution of software from BSLM.

1.2.6.7.1. Provide Memo For Record (MFR) and process IAW licensing and/or purchasing agreements.

1.2.6.7.2. Retain completed MFR for audit trail of disposed assets.

1.2.7. Route request for extension on annual requirement suspense to the BSLM through the Unit APO. Extension requests not routed through the Unit APO may be disapproved.

1.2.8. CST will:

1.2.8.1. Assist USLM with software inventories as required.

1.2.8.2. Ensure illegal copies of copyrighted software are not made.

1.2.8.3. Ensure software is not installed without approval from USLM.

1.2.8.3.1. All software installs require USLM approval unless it is in the BSLM designated “no approvals needed" network location.

1.2.8.3.2. BSLM will provide a list of all designated network locations where approvals are not required.

1.2.8.4. Notify the USLM if users appear to have installed software applications without USLM approval.

1.2.9. IT Hardware Asset Users: Users are responsible for the overall safeguarding and welfare of IT hardware assets under their control. In addition, users will:

1.2.9.1. Maintain a clean and secure environment for their assigned IT hardware assets.

1.2.9.2. Not relocate any IT hardware asset without prior approval from their PC.

1.2.9.3. Notify their PC immediately if a piece of equipment is lost, stolen, or damaged.

1.2.9.4. Not attempt to repair, upgrade IT hardware assets.

Chapter 2

HARDWARE ASSET MANAGEMENT

2.1. Control Measures.

2.1.1. Per AFI 23-111, *Management of Government Property in Possession of the Air Force*, Personnel having custodial responsibility may incur pecuniary liability for the loss, destruction, or damage to property caused by willful misconduct, deliberate unauthorized use, or negligence in the use, care, custody, or safeguard of the property from causes other than normal wear and tear. There are two methods to establish custodial responsibility:

2.1.1.1. Unit Accountable Property Officer appointment of a Property Custodian.

2.1.1.2. The use of hand receipts.

2.1.1.2.1. Hand receipts may be AF Form 1297, *Temporary Issue Receipt.*

2.1.1.2.2. If the AF IMT 1297 is not used, the electronic hand receipt or automated system must state, "I acknowledge receipt of and responsibility in accordance with AFI 23-111 for the items described below and will return them by the return date indicated."

2.1.1.2.3. All hand receipts must be signed and contain the signer's contact information.

2.1.2. Physical or automated inventories will be completed no later than 365 days from the date the last inventory was signed by the Unit APO. The Unit APO will certify accuracy and completion of all inventories by endorsing them.

2.1.2.1. Any IT assets determined to be lost, stolen, or damaged (whose manufacturer's warranty will not repair or replace) must be reported to the responsible Unit APO and ECO within 5 duty days of determination via the FLI process utilizing the DD Form 200 or Tinker Form 34, *Inventory Adjustment Form*.

2.1.2.2. Before turning into the ITAM office for processing, completed inventories must contain active FLI numbers or Tinker Form 34 annotated next to each asset determined to be lost, stolen, or damaged (whose manufacturer's warranty will not repair or replace).

2.1.3. PCs will submit an Annual Requirements Package consisting of their official inventory (will initially receive an inventory spreadsheet to be updated and returned to the ITAM Office), an updated appointment letter (using the latest template from the Tinker ITAM SharePoint site) and training certificates for both the primary PC and alternate PC to the ITAM Office by the 10th of the month their annual requirements are due. All documents, within the package, will be signed, dated, and completed within the same calendar month.

2.1.3.1. Partial packages will be returned to the PC to hold until all requirements are complete.

2.1.3.2. Loss/Gain packages, used to transfer primary PC responsibilities, will also have all documents signed, dated, and completed within the same calendar month.

2.1.4. The ITAM office will notify PCs, OCMs, and appropriate organizational workflows 30 – 45 days prior to their annual requirements suspense date. The annual requirement suspense date will be determined by using the previous annual inventory's Unit APO signature date.

2.1.4.1. If annual requirements are not received by the set suspense date, an initial elevation email will be sent to the Division/Squadron Commander. If no resolution has occurred after seven (7) calendar days a second elevation email will be sent to the Directorate/Group Commander. If after 14 calendar days, resolution has not occurred, a third elevation email will be sent to the Wing Commander.

2.1.5. Overdue ITAM accounts will be frozen in the designated APSR and new purchases disallowed until the account is compliant. All transactions (i.e., additions, transfers, etc.) will be suspended until the account is compliant. The only exceptions will be for transactions necessary to produce an accurate inventory.

2.2. Purchasing Procedures.

2.2.1. End-user devices can be tech-refreshed IAW recommended frequency outlined in accordance with DAFMAN 17-1203.

2.2.1.1. When an organization receives a replacement IT asset for a technical refresh or replaces an unserviceable asset, the owning PC will coordinate with the ECO, and the Information System Security Office (ISSO) or wing Information Assurance (IA), in order to process the disposal to DLADS. (T-1). Once DLADs has received the asset and completed the turn in, the ECO will remove the asset from the APSR within 30 calendar days.

2.2.2. Central Procurement of IT Assets: IT Assets will be procured through an Air Force managed program, i.e., Quantum Enterprise Buy (QEB) using Client Computing Solutions III (CCS-3), Digital Imaging and Printing (DPI) or Blanket Purchase Agreement (BPA). Unit APO's will ensure acquisitions are submitted and approved IAW current 72d Communications Directorate guidance.

2.2.2.1. All IT purchases will contain accurate information for shipping labels.

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

2.2.2.1.2. "Ship To" information will contain the complete delivery address. This includes the ECO and Property Custodians' names.

2.2.2.2. IT purchases not containing accurate information on shipping labels will result in delayed processing time and end-users will experience a delay in receiving their purchased IT equipment.

2.2.3. Central Delivery of all IT Hardware Assets: All IT hardware asset purchases will be delivered to the ECO, ITAM Centralized Warehouse, for receipt and processing. Contact the ECO for the current ITAM Centralized Warehouse address. Exceptions must be coordinated with the ECO during the requirements phase of the purchase.

2.2.3.1. PCs will be notified, by the ITAM warehouse personnel, when assets are available for pickup and must be retrieved within 5 business days of notification. Failure to pick up assets will result in an elevation email to PC leadership.

2.2.3.2. Upon pickup of newly received assets PCs will create a turn-in appointment with the Dispositions Office ensuring a one for one swap occurs within 30 calendars of receiving new assets.

Chapter 3

SOFTWARE ASSET MANAGEMENT

3.1. Control Measures.

3.1.1. BSLM will review account status bi-monthly for overdue accounts and notify USLM of non- compliance. Account compliance is determined by the current year appointment letter, Primary and Alternate USLM training certificates, and annual account inventory.

3.1.1.1. Initial notification email will be sent to the current appointed USLM 45 days prior to account's static month due date. All USLM accounts have an assigned static month and inventories are due by 15th of the static month (if falls on a weekend or holiday, will be the next business day).

3.1.1.2. A reminder email from the BSLM will be sent to the USLM and the USLM's supervisor if no account documents are submitted by the account's static due month date. USLM's will be given a 7-calendar day suspense to comply and if no resolution occurs the BSLM will initiate an elevation process.

3.1.1.3. If no resolution occurred, a first level elevation email will be sent to the Division/Squadron Commander with a 14-calendar day suspense to comply. If no resolution has occurred, a second level elevation email will be sent to the Directorate/Group Commander with a 14-calendar day suspense to comply. If there are still no resolutions occurred, a third level elevation email will be sent to the Wing Commander with a 14-calendar day suspense to comply.

3.1.2. BSLM will lock accounts when first level elevation occurs. Locked accounts are affected by the following:

3.1.2.1. Software purchases are placed on hold

3.1.2.2. Software installs requiring USLM/BSLM approval will be denied.

3.1.2.3. Non-Enterprise software may be removed from USLM account to ensure compliance with this instruction and DAFMAN 17-1203.

3.2. Tinker AFB Software Licensing Program Processes.

3.2.1. COTS/IUS Software must be purchased through approved enterprise software initiative procurement sources, if applicable.

3.2.2. BSLM will determine the required acquisition source(s), if applicable.

3.2.3. Required sources are listed in DAFMAN 17-1203.

3.3. Software Receiving.

3.3.1. Receipt procedures. USLM must match receipts to a fully approved work order, or current 72 ABW/SC directed process, and all new software media/licenses which must be stored at the Enterprise Information Management (EIM) site designated by BSLM. The BSLM may designate an alternate electronic storage method for software license management working level documentation.

3.3.2. Before installing newly acquired software the above receipt procedures must be completed in its entirety.

3.3.3. Physical receiving. The USLM shall receive all physical media.

3.3.4. Electronic receiving. The USLM shall download all electronically delivered software from approved websites. If USLM is unable to download due to it being inaccessible over the network, the USLM needs to call in a help ticket to request the software be downloaded with the help of the Comm Focal Point.

3.4. Software Transfer.

3.4.1. Software license transfers between USLM accounts must be accomplished with the appropriate software transfer form Tinker Form 335, *Software Transfer Request*, and uninstalled from the losing accounts computers.

3.4.2. USLM will send BSLM a copy but ultimately maintains final software transfer form, Tinker Form 335, in their EIM folder, account folder, and local Tinker Electronic Records Management System (ERMS) site.

ABIGAIL L.W. RUSCETTA, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DAFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM),* 13 Sep 2022 AFI 33-322, *Management of Records,* 06 March 2022

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

AFI 38-101, *Air Force Organization,* 31 January 2017

DoDI 5000.64, *Accountability and Management of DoD Equipment and Other Accountable Property*, 27 April 2017

DoD FMR–7000.14-R Volume 12, Chapter 7, *Special Accounts, Funds and Programs,* 7 March 2014

AFI 63-101/20-101, *Integrated Life Cycle Management,* 09 May 2017

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

Prescribed Forms

Tinker Form 30, *Accountable Asset Add or Government Purchase Card (GPC)*

Tinker Form 32, *Computer System Equipment Action*

Tinker Form 34, *Inventory Adjustment Form*

Tinker Form 335, *Software Transfer Request*

Adopted Forms

AF 847, *Recommendation for Change of Publication*

AF IMT 1297, *Temporary Issue Receipt*

Abbreviations and Acronyms

AFB—Air Force Base

AFEMS—Air Force Equipment Management System

AFNet—Air Force Network

AFRIMS—Air Force Records Information Management System

APO—Accountable Property Officer

APSR—Accountable Property System of Record

AUIC—Accountable Unit Identification Code

BPA—Blanket Purchase Agreement

BSLM—Base Software License Manager

COTS—Commercial Off-The-Shelf

CST—Client System Technician

DLADS—Defense Logistics Agency Disposition Services

ECO—Equipment Control Officer

EIM—Enterprise Information Management

ERMS—Electronic Records Management System

EULA—End User License Agreement

FLI—Financial Liability Investigation

GPC—Government Purchase Card

IAW—In Accordance With

IT—Information Technology

ITAM—Information Technology Asset Management

IUID—Item Unique Identification

IUS—Internal Use Software

JA—Judge Advocate

MFR—Memorandum for Record

MICT—Management Internal Control Toolset

OCM—Organization Computer Manager

OPR—Office of Primary Responsibility

PC—Property Custodian

QEB—Quantum Enterprise Buy

RDS—Records Disposition Schedule

SAV—Staff Assist Visits

SLM—Software License Management

TDY—Temporary Duty

UAPO—Unit Accountable Property Officer

UIC—Unit Identification Code

USLM—Unit Software License Manager

VoIP—Voice Over Internet Protocol

Attachment 2

PILFERABLE ITEM WORKSHEET

Figure A2.1. Pilferable Item Tracking Spreadsheet.

Custodian Name:		**Owning Org/Off:**											
Pilferable Item Definition:													
	Acq Cost	**Desc**	**Ldgr**	**Loc**	**Model #**	**N S N**	**Part #**	**Serial # or UII**	**Svc Date**	**Status**	**Qty**	**Useful Life**	**U/I**
1													
2													
3													

Figure A2.2. Pilferable Item Tracking Spreadsheet Directions.

Pilferable Item Tracking Spreadsheet Directions	
Acq Cost:	Initial acquisition cost and depreciation information, if applicable; or original acquisition cost if the property does not require capitalization
Custodian Name:	Individual accountable for managing pilferable assets
Desc:	Description (e.g., noun, nomenclature) of asset
Ldgr:	General ledger classification (e.g., general equipment, loaned or leased, or a means to apply business rules for making such a determination)
Loc:	DoD activity address code, unit identification code, commercial and government entity code
Model #:	Model Number of asset
NSN:	National stock number (if known)
Owning Org/Off:	Current owning Organization/Office symbol
Part #:	Part Number of asset
Pilferable Item Definition:	Unit APO defined parameters of Pilferable assets to be managed
Qty:	Received, Fabricated, Issued, or On-Hand
Serial # or UII:	Serial Number or Unique item identifier or DoD recognized IUID equivalent as defined in DoDI 8320.04 of asset
Svc Date:	Date asset was placed in service
Status:	Active or Inactive/Retired (e.g., Staged, Stored, In-Transit, Transferred, Declared Excess, Awaiting Disposition, or Dispositioned)
U/I:	Unit of measure
Useful Life:	Estimated useful life (years or activity based for capitalized property)