BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 17-1203

19 MARCH 2014
Incorporating Change 2, 7 March 2017

Communications and Information

INFORMATION TECHNOLOGY (IT)
ASSET MANAGEMENT (ITAM)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/CIO A6SE

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

Supersedes: AFMAN33-153, 19 March 2014, AFI33-112, 7 January 2011 and AFI33-114, 13 May 2004

Pages: 50

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; AFPD 63-1/20-1, Integrated Life Cycle Management; and AFPD 10-6, Capabilities-Based Planning & 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) and maintaining accountability of Personal Wireless Communications Systems (PWCS) including cellular telephones and pagers. The software management guidance identifies responsibilities for management of commercial off-the-shelf (COTS). 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, 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 alternately, to the Publication OPR for non-tiered compliance items. 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 interim changes revises AFMAN 33-153 by (1) adding mandatory NETCENTS-2 use for all IT procurements, (2) adding tiering to ITEC/PEC rank/grade requirements, (3) allowing optional use of AFEM-AIM for non-sensitive IT asset tracking. A margin bar (|) indicates newly revised material.

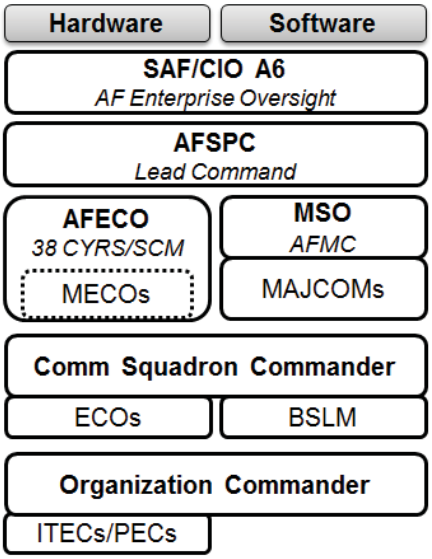
Chapter 1

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 PWCS. Refer to AFI 33-590, *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; see AFPD 63-1/20-1). 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.

1.2. Roles and Responsibilities. Figure 1.1 below represents an overview of those IT Asset Management roles and responsibilities from the AF to the organizational level.

Figure 1.1. IT Asset Management Roles and Responsibilities Overview.



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 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 formal ITAM and software management training requirements and provides them to Headquarters Air Education and Training Command (AETC/A3T) for incorporation into formal courses or long-distance learning approaches.

1.2.1.4. 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.

1.2.1.5. 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.

1.2.1.6. Serves as the AF software license manager to review and consolidate the AF software license inventory in coordination with Air Force Space Command (AFSPC) as lead command. MAJCOM and base inventories include locally-owned software and software not yet transferred to an enterprise software license agreement.

1.2.1.7. 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.

1.2.1.8. Ensures warfighting systems software compliance with DoD Directive (DoDD) 8320.02, *Data Sharing In A Net-Centric Department of Defense*.

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

1.2.2.1. Special Access Programs (SAP) IT hardware assets will be tracked in the Air Force Equipment Management System Asset Inventory Management (AFEMS-AIM), or other approved accountable systems of record for accountability of hardware. 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 the AFEMS-AIM will be separately tracked within the SAP configuration control project databases. All assets considered an operational node in cyberspace will be tracked for accountability.

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 in accordance with Department of Defense Instruction (DoDI) 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information*, AFPD 33-2 and AFI 33-200, *Information Assurance (IA) Management*. In accordance with Intelligence Community Directive (ICD) 503, granted by the Director of National Intelligence, relevant national Intelligence Community (IC) elements, and DoD, AF/A2 may formally

delegate specific duties, roles, and responsibilities for providing policy and oversight for IT assets, including hardware assets, as well as software procured outside of AF Enterprise Licensing or COTS products on the AF Evaluated/Approved Products Listing (E/APL).

1.2.3.2. AF IT hardware assets under the cognizance of AF/A2 will be tracked in AFEMS-AIM, or other approved accountable systems of record for accountability of hardware. The cognizant security authority representative will evaluate all security issues and concerns before rendering a determination as to which assets will be tracked. AF/A2 or designated representative will provide guidance for meeting regulatory compliance for IT hardware assets not tracked in AFEMS-AIM.

1.2.4. **Air Force Space Command (AFSPC).**

1.2.4.1. Serves as lead command for implementation of ITAM and software management policies.

1.2.4.2. Develops and implements the AF-wide IT hardware and software management system to provide for an AF Configuration Management Database (CMDB). The CMDB will contain all AF hardware inventory, infrastructure configuration information, COTS entitlements, and software implementation metrics.

1.2.4.2.1. Assures IT asset inventory information is associated and/or synchronized to provide the complete picture of the IT asset life cycle between the CMDB, AFEMS-AIM, acquisition purchasing databases, financial databases, and any other systems requiring an authoritative data source for IT asset information.

1.2.4.2.2. Coordinates with Air Education and Training Command (AETC) to ensure proper training is established to ensure end users of the CMDB can utilize the database and subsequently fulfill their oversight responsibilities.

1.2.4.2.3. The CMDB enables AF implementation of the Information Technology Infrastructure Library (ITIL) practices for Software Asset Management in accordance with International Standardization Organization/International Electrotechnical Commission (ISO/IEC) 20000, *Information Technology - Service Management*.

1.2.4.2.4. The CMDB supports AF Configuration Management as directed by AFI 33-115 to be published as *AF IT Services*. This complements ISO/IEC 19770, *Software Asset Management (SAM).*

1.2.4.3. Publishes to DoD ITAM and software metrics for IT hardware (including PWCS), and software entitlements and implementation.

1.2.4.4. Manages the AF E/APL and publishes to the AF Portal the certified COTS Software Products for use on AF networks.

1.2.4.5. Coordinates with SAF/CIO A6, AFMC's Managed Services Office (MSO) and MAJCOMs for software license requirements and consolidates non-enterprise software inventories.

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 AFEMS-AIM.

1.2.5.2. Provides guidance and support to MAJCOMs, FOAs, and DRUs in managing 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. Acts as ITAM functional manager for AFEMS-AIM for all proposed upgrades and/or modifications to AFEMS-AIM.

1.2.5.4.1. Maintains the list of designated Major Command Equipment Control Officers (MECOs) and Base/Tenant IT Equipment Control Officers (ECOs).

1.2.5.4.2. Manages AFEMS-AIM accounts for ECOs, to include approving new account requests and freezing noncompliant AFEMS-AIM accounts.

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 (MOAs) governing the transfer of A6 workload responsibilities to AFSPC, (T-1).

1.2.5.6. Approves asset transfers between commands when serving as the MECO.

1.2.5.7. 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 for all IT hardware assets managed in AFEMS-AIM.

1.2.5.8. Provides management guidance to Air Force Medical Operations Agency (AFMOA/SGAL) for medical War Reserve Material (WRM) IT hardware assets accounted for in Defense Medical Logistics Standard Support (DMLSS).

1.2.5.9. **(ADDED)** Has authority to freeze a Defense Reporting Activity (DRA) 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. Develops and executes comprehensive training plans and materials that addresses all aspects of ITAM and software management as requested by SAF/CIO A6.

1.2.7.2. Provides training through centrally-managed, computer-based training courses or other distance learning approaches.

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

1.2.8.1. Appoints a MAJCOM ECO (MECO), documents acknowledgement of duties with handwritten or digital signatures, and provide a copy to the AFECO. Exception: 38

CYRS will assign a MECO if they are performing MECO duties required by MAJCOM MOAs governing the transfer of A6 workload responsibilities to AFSPC, (T-1).

1.2.8.2. Notify 38 CYRS/SCM (38CYRS.ITAM@us.af.mil) when the MECO changes.

1.2.8.3. Ensures all COTS license requirements are purchased using approved DoD/AF Enterprise Licenses Agreements (ELAs), DoD ESI or approved contract vehicle as identified in paragraph 3.2, (T-1).

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

1.2.9.1. Be responsible for the overall management of the MAJCOM, DRU, FOA, or Equivalent IT hardware asset management program and management of assigned ECOs. Provide guidance and procedures to the ECOs on management of IT hardware assets, (T-1).

1.2.9.1.1. Have a recommend minimum grade of E-7/GS-11 for this position and prior ECO experience is recommended.

1.2.9.1.2. Not be the ECO for any Defense Reporting Activity (DRA) in the same command according to DoD *Financial Management Regulation* (DoDFMR) 7000.14-R, Volume 1, **Chapter 3**, *Federal Financial Management Improvement Act of 1996 Compliance, Evaluation, and Reporting* and AFPD 65-2, *Managers' Internal Control Program*, (T-0).

1.2.9.2. Maintain the list of designated ECOs, (T-1).

1.2.9.3. Coordinate with other MECOs to establish tenant units reporting procedures and problem resolution, (T-2).

1.2.9.4. Approve or reject transfer of IT hardware assets between commands and coordinate with losing/gaining MECO, (T-1). The AFECO will serve as a mediator when problems arise.

1.2.9.5. Approve or reject excess IT asset reports completed by ECOs and ensure appropriate action is accomplished, (T-1).

1.2.9.6. Allow ECOs to create and maintain holding accounts for known near-term requirements, as required, (T-2).

1.2.9.7. Provide assistance to ECOs for establishing new DRAs, closing out a DRA (e.g., base closures), or IT data system connectivity requests, (T-1).

1.2.9.8. Freeze DRAs for failure to comply with directions or procedures. This option should only be utilized after providing the ECO an opportunity to correct any deficiencies in a timely manner due to the potential for serious impact to an organization's mission, (T-2).

1.2.9.9. Provide AFEMS-AIM reports to ECOs, Communications Squadrons, MAJCOM A6 or MAJCOM Inspection Teams, upon request. Reports can include overdue inventories, reports of surveys, aging assets, disposal transactions, etc., (T-2)

1.2.9.10. Complete additional training as directed by the AFECO.

1.2.10. **Communications Squadron (CS) Commander, Director, or Equivalent.** Each communications squadron commander/director will:

1.2.10.1. Serve as the accountable officer for all IT hardware equipment listed in their assigned DRA, (T-2).

1.2.10.1.1. 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).

1.2.10.1.2. Optionally appoint a separate primary and alternate PWCS ECO according to ECO guidance. ECOs may serve as PWCS ECOs. (T-3)

1.2.10.1.3. Ensure the AFEMS-AIM inventory provides accountability of all IT hardware assets assigned to that DRA, (T-1).

1.2.10.1.4. DELETED.

1.2.10.1.5. Assume accountability/responsibility for all AF enterprise assets located on each installation (e.g. gateway equipment, network infrastructure, defensive sensors, core service servers). The owning MAJCOM and/or organization will be identified on the asset record, (T-2).

1.2.10.1.6. Direct the use of Hand Receipts (i.e. AF Form 1297, *Temporary Issue Receipt*), or automated process that meets the intent, as necessary for inventory control, (T-2).

1.2.10.1.7. Establish accountability of hardware assets for all base IT orders, (T-2).

1.2.10.1.8. **(ADDED)** If responsible for a DRA managed by an ECO, ensures 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.)

1.2.10.2. Designate primary and alternate BSLMs (or equivalents) to manage the wing and/or base software license programs (to include applicable tenants) and inform their MAJCOM/A6 and AFSPC/A6 as lead command, (T-1).

1.2.10.2.1. Ensure all BSLMs (or equivalents) complete any available software license management training, (T-3).

1.2.10.2.2. 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 AFSPC/A6 as lead command, (T-1).

1.2.10.3. Assist organizational commanders and contracting officers (COs), to ensure all hardware and software is purchased according to **paragraph 2.2** for hardware and **paragraph 3.2** for software, (T-1).

1.2.10.3.1. As required, assist the supporting contracting officers (COs) in determining requirements and developing an acquisition strategy for maintenance contracts in support of **Chapter 2 Section 2B**, (T-3).

1.2.10.3.2. Provide technical/functional expertise, advice, and support to COs for preparing request for quotation (RFQ), RFQ response review, solicitation, and source selection actions, (T-3).

1.2.10.3.3. Adhere to budgeting agreements and arrangements established in Host Tenant Support Agreements (HTSAs), (T-3).

1.2.10.4. Assist organizational commanders or equivalents in developing consolidated cost-effective IT hardware asset maintenance solutions across the installation(s), (T-3).

1.2.10.4.1. Manage and direct retention of serviceable excess IT hardware assets, when allowed by the MECO, for maintenance redundancy or operational spares, by maximizing use of sharing and redistribution to meet user requirements.

1.2.10.4.2. Authorize cannibalization of IT hardware assets to satisfy critical mission requirements and spare parts according to **Chapter 2** (Consider warranty status prior to cannibalization).

1.2.10.5. Ensure HTSA directs all base units to participate in the host-base software license management program if they are AF organizations connected to AF local area networks, (T-3).

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

1.2.11.1. Is appointed as primary or alternate by the CS Commander (or equivalent), (T-1). According to DoDFMR 7000.14-R, Volume 1, **Chapter 3** and AFPD 65-2, the ECO cannot be the Property Custodian for any AFEMS-AIM account other than an account established for holding assets prior to distribution or disposal (i.e. holding or excess accounts), (T-0). All normal account management requirements apply (i.e. appointment letters, annual inventory, etc.) to these holding accounts.

1.2.11.1.1. ECOs should have the leadership skills and IT asset knowledge necessary to provide guidance and direction to the Property Custodian regarding IT asset management.

1.2.11.1.2. The minimum rank/grade requirement for the primary ECO is E-5 or civilian equivalent, (T-3). There is not a rank/grade requirement for an alternate ECO.

1.2.11.1.3. If contractor employees are assigned to perform ECO duties under the terms of a contract, the AF retains responsibility for obligating funds and receiving assets as they are inherently governmental functions according to Federal Acquisition Regulation (FAR) Subpart 7.5, *Inherently Governmental Functions*.

1.2.11.1.4. In deployed locations, the forward commander appoints a qualified individual available to perform the duties of ECO.

1.2.11.1.5. ECOs will clear all tasks in the AFEMS-AIM system and notify MECOs via email for out-processing approval.

1.2.11.1.6. If accountable for PWCS, completes PWCS Manager Training, using AETC approved training materials, within 90 days of appointment. If PWCS manager training materials are unavailable for use within the initial 90-day appointment period, contact AFECO (38 CYRS/SCM PWCS MECO) to obtain guidance on available alternate training options such as Staff Assistance Visits, MAJCOM qualification training packages, or computer-based training.

1.2.11.1.7. Complete additional training as directed by the AFECO.

1.2.11.1.8. **(ADDED)** The ECO cannot be appointed Resource Advisor (RA) within the same unit in which they are performing duties as ECO, (T-1).

1.2.11.2. Provide guidance and annual training for Property Custodians regarding IT asset management, (T-2).

1.2.11.2.1. Maintain listing of Property Custodian appointments, (T-2).

1.2.11.2.2. Annual training must be documented in AFEMS-AIM and a review of training currency should coincide with the annual inventory, (T-2).

1.2.11.2.3. Training, at a minimum, will include Property Custodian roles and responsibilities as they pertain to IT asset management, as well as any local policies for disposal, training, new item adds, etc., (T-2).

1.2.11.2.4. Complete out-processing for departing Property Custodian upon transfer of account; requires assignment of new Property Custodian and certified joint loss-gain inventory of IT assets, (T-2).

1.2.11.3. The ECO is responsible for all management of equipment listed in his/her assigned DRA, (T-1). The ECO will process the receipt and transfer of all IT assets and complete necessary documentation to establish custodial responsibility according to **Chapter 2**, (T-1).

1.2.11.3.1. Assist Property Custodians in determining the ownership, reassignment or disposition of all Found-on-Base (FOB) IT assets, (T-2).

1.2.11.3.2. Direct Property Custodians to conduct annually, at a minimum, a complete inventory of all IT hardware assets and/or PWCS assigned to the Property Custodian's AFEMS-AIM account, (T-1).

1.2.11.3.3. Provide Property Custodians with AFEMS-AIM generated, IUID or equivalent labels, see paragraph 2.3.1.6., (T-1).

1.2.11.3.4. DELETED.

1.2.11.3.5. Deploy AFEMS-AIM accountable, Unit Task Code (UTC) tasked IT assets at the request of the Property Custodian or deployment authority. AFEMS-AIM will be used to accomplish the deployment, (T-2).

1.2.11.3.6. Attempt to reutilize excess IT assets that meet minimum network configuration standards before offering equipment to organizations outside the DRA, when allowed by the parent MAJCOM, (T-2).

1.2.11.3.7. After receipt of a transportation fund site, if applicable, direct the losing custodian to prepare the necessary shipping documents for items that are excess and required by other services, (T-3).

1.2.11.3.8. Coordinate with any tenant ECO to establish an HTSA identifying any assistance required, such as AFEMS-AIM connectivity, (T-2).

1.2.11.3.9. Coordinate on all HTSAs concerning IT asset management. IT accountability support can be specified in the HTSA or a MOA, (T-2).

1.2.11.3.10. Unless otherwise directed, may develop and mandate use of locally-generated products and/or forms by the Property Custodian to ensure accurate documentation and data entry for the addition, transfer, deletion, or disposal of IT assets.

1.2.11.3.11. Monitor AFECO collaboration sites for additional guidance and support.

1.2.11.3.11.1. ITAM - **https://cs3.eis.af.mil/sites/OO-SC-CA-45/default.aspx**.

1.2.11.3.11.2. PWCS - **https://cs3.eis.af.mil/sites/OO-SC-CA-32/default.aspx**.

1.2.11.3.12. Perform periodic compliance visits to ensure accountability and asset management processes are effective. Educate and assist Property Custodian with development of corrective actions. For PWCS assets, refer to section 3.10 of AFI 17-210 for further instructions.

1.2.12. **Base Software License Managers (BSLM) (or equivalents).** Each BSLM (or equivalents) will:

1.2.12.1. Ensure each organization maintains a software inventory of all non-enterprise Government off-the-shelf software (GOTS)/COTS and associated licenses used by the organization, (T-2). Maintain a current list of all designated organization representatives.

1.2.12.2. Ensure annual inventories are conducted for all non-enterprise software licenses for all organizations under BSLM purview, (T-1).

1.2.12.2.1. Monitor each organization's automated software inventories.

1.2.12.2.2. Collect an annual baseline of an inventory for all non-enterprise software licenses which is certified by each organizational commander/director.

1.2.12.2.3. Provide annual inventories to higher headquarters as required or requested. If requested, assist with providing enterprise software licensing inventory.

1.2.12.3. DELETED

1.2.12.4. Provide software license training for Client Systems Technicians (CSTs), helpdesks, and any other personnel managing software licenses according to **Chapter 3**, (T-2).

1.2.12.5. Perform periodic compliance visits to base units and tenant organizations with any non-enterprise software that is not automatically monitored according to **Chapter 3**. Refer to AFI 90-201, *The Air Force Inspection System*, and the IT Asset Management checklist in the Management Internal Control Toolset (MICT) for software inspection criteria and guidance, (T-3).

1.2.12.6. Verify new acquisitions against the procedures in **paragraph 3.2**, (T-1).

1.2.13. **Organizational Commanders or Equivalent.** 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:

1.2.13.1. In coordination will local communications squadron (or equivalent), budget for and procure IT hardware (including PWCS) and software including maintenance within your organizational responsibility according to **paragraph 2.2** for hardware and **paragraph 3.2** for software, (T-1).

1.2.13.2. Review organization's IT hardware (including PWCS) and software requirements documents and submit IT requirements to the applicable CS (or equivalent) for technical solutions and enterprise buy options, (T-2).

1.2.13.3. Appoints a minimum of one primary and one alternate property custodian for IT asset management. Appointments will occur no later than 45 calendar days prior to the projected departure of the current Property Custodian, (T-2). Appointment letters will be reviewed annually and a new appointment letter will be completed if there have been personnel changes.

1.2.13.3.1. Forward the appointment letter and request for any IT asset-specific training to the ECO, (T-2).

1.2.13.3.1.1. The appointment letter must be dated and must contain the names and written or digital signatures of the primary and alternate Property Custodian acknowledging their appointment as manager of IT assets.

1.2.13.3.1.2. Ensure Property Custodian(s) are scheduled for training with the ECO within 30 calendar days of initial appointment and annually thereafter.

1.2.13.3.2. Ensure departing Property Custodian(s) out process through the ECO, (T-2).

1.2.13.4. Ensure the Property Custodian accounts for all IT hardware assets by performing annual and/or out-of-cycle inventories according to **Chapter 2**, (T-1).

1.2.13.5. Review assigned IT hardware assets annually. Determine if the IT is obsolete, still meets user requirements or needs modification. Further, determine if IT hardware is unused or underutilized to comply with E.O. 13589, *Promoting Efficient Spending*. After replacement, obsolete IT hardware assets will be coordinated for disposal with the ECO.

1.2.13.6. Manage all software licenses owned by the organization in support of the base software license management program according to **Chapter 3**, (T-1). The inventory of software licenses at the organization level includes those software licenses that are managed by enterprise software licensing agreements when requested.

1.2.13.6.1. Annually certify and document to the BSLM a software inventory was accomplished, (T-3).

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

1.2.13.6.3. 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-2).

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

1.2.13.8. 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).

1.2.13.9. Coordinate all software acquisitions through the respective BSLM (or equivalents) prior to purchasing software, (T-1).

1.2.13.10. **(ADDED)** If responsible for a DRA managed by an ECO, ensures 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.)

1.2.13.11. **(ADDED)** Determines ROS eligibility per section 2.5.13.

1.2.14. **IT Equipment Custodian (ITEC) and/or PWCS Equipment Custodian (PEC).**

1.2.14.1. Appointed by the organization commander (or equivalent).

1.2.14.1.1. The primary property custodian managing IT assets must be commissioned officers, NCOs, warrant officers, contractors (as specified in the contract), or civilians (minimum civilian grade is GS-5, NAF-III or other equivalent civilian pay grade series). Local wage rate (LWR) employees (foreign employees in host countries) may be appointed primary Property Custodian for IT assets ONLY if the host country's law's hold them financially liable, (T-1). There is not a rank/grade requirement for alternate Property Custodian for IT assets. Drill Status Guardsmen and Reservists are not recommended to serve as Property Custodians for IT assets due to their limited work availability.

1.2.14.1.2. DELETED.

1.2.14.1.3. Contractors may also be ITECs/PECs according to the provisions **Chapter 2** and AFI 23-111, *Management of Government Property in Possession of the Air Force,* if allowable under the contract terms and conditions and approved by the organization commander and the CS.

1.2.14.1.4. Foreign nationals or local wage rate employees (foreign nationals in host countries) as primary or alternate ITECs/PECs may be approved by the commander and the CS only when they may be held pecuniary liable for losses of equipment under the law of the host country and according to the provisions of AFI 31-501, *Personnel Security Program Management*, AFI 33-200 and AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program*.

1.2.14.2. Accountable for all assigned IT hardware assets and PWCS assets.

1.2.14.3. Performs, at a minimum, an annual inventory of all IT assets in the AFEMS-AIM account, (T-1).

1.2.14.4. Ensure all accountable assets have AFEMS-AIM generated, IUID or equivalent labels affixed according to **paragraph 2.3.1.6.3**, (T-2).

1.2.14.5. Notifies ECO of all shipments (incoming and outgoing), transfers, donations, or turn-ins of excess IT assets, (T-2).

1.2.14.6. Provides appropriate documentation to the applicable ECO to clear the account of IT equipment that was shipped to another base/location, transferred to another account, donated to a school, or turned in to the Defense Logistics Agency Disposition Services (DLADS). This includes IT hardware assets DLADS identifies as being donated to schools under the Computers for Learning (CFL) program, (T-2).

1.2.14.7. Must be approved to out-process by the applicable ECO, (T-2).

1.2.14.8. Conducts a loss-gain joint inventory in accordance with section 2.5.5.2.

1.2.14.9. Upon discovery of lost, damaged, or destroyed assets, (T-1):

1.2.14.9.1. Notify the ECO and organization commander or equivalent

1.2.14.9.2. Report the loss of any IT hardware asset with persistent storage to the ISSO or wing IA according to requirements outlined in AFI 33-200 and AFI 31-401, *Information Security Program Management*, and any local procedures.

1.2.14.9.3. DELETED.

1.2.14.10. Provide the applicable ECO with a serialized numbered list of any AFEMS-AIM accountable UTC-tasked assets considered for deployment, (T-2).

1.2.14.11. Ensure hard drives are sanitized according to the procedures outlined in AFMAN 33-282, *Computer Security (COMPUSEC)*, (T-0).

1.2.14.12. Cellular devices must be disposed of IAW applicable National Information Assurance Partnership Protection Profiles (NIAP PPs) or Security Technical Implementation Guides (STIGs). In cases where those documents do not specify disposal procedures, devices must be sanitized with a National Security Agency (NSA) approved method/product before being transferred outside the AF, (T-0).

1.2.14.13. Excess cellular devices exposed to classified information must be turned in to DLADS for destruction. Before sending cellular devices to DLADS for destruction they shall be wiped based on the NIAP PP or STIG, (T-0).

1.2.15. **Client Systems Technician/Helpdesk Responsibilities (CST).** Each Client Systems Technician/Helpdesk will:

1.2.15.1. Not purchase, obtain, or install hardware or software without prior coordination with the applicable ECO, Property Custodian, or BSLM, (T-3).

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

1.2.15.3. Ensure all networked computer systems are in compliance (i.e., installed and managed by Group Policies) with the AF Standard Desktop Configuration (SDC), (T-1).

1.2.15.4. Ensure limited user access/permissions on computer systems are imposed and maintained to enforce AF SDC integrity, (T-1). This may be accomplished by using an automated software tool to ensure administrator rights are removed.

Chapter 2

HARDWARE ASSET MANAGEMENT

Section 2A—Hardware Assets Accountability and Reporting

2.1. Accountability of IT Hardware Assets and Inventory Management.

2.1.1. **Accountability Determination.** The accountability of hardware assets is governed by multiple and complex congressional, federal, DoD, and AF policies. Hardware assets may be hybrid devices with multiple uses complicating the clear definition of a specific hardware type. The following paragraphs will be used to determine accountability of AF IT assets based on acquisition cost thresholds and features of the hardware.

2.1.1.1. Send concerns about the inclusion or exclusion of IT hardware assets in AFEMS-AIM to 38 CYRS/SCM (**38CYRS.ITAM@us.af.mil** or DSN 779-6280).

2.1.1.2. Refer to AFI 90-201, *The Air Force Inspection System*, and the IT Asset Management checklist in the Management Internal Control Toolset (MICT) for hardware and software inspection criteria.

2.1.2. **Sensitive IT Assets (Controlled Inventory Items).**

2.1.2.1. Sensitive IT assets are any IT hardware with persistent storage (e.g. laptop, desktop, server, tablet, smartphone, external hard drive, and thumb drive) or are Internet Protocol (IP) network capable (e.g. thin client, network printer, router, switch, and VoIP phone). Persistent storage does not include device firmware. IP network capability does not include Wireless Personal Area Network (WPAN) capabilities lacking IP network features (e.g. Bluetooth, RF, and infrared).

2.1.2.2. Sensitive IT assets must be accounted for in AFEMS-AIM as commodity code "A" due to their capability to process and/or transmit personally identifiable information or other sensitive agency information according to DoDI 5000.64, *Accountability and Management of DoD Equipment and Other Accountable Property*. Physical accountability of these items is required in support of IT configuration management and information assurance requirements. Physical accountability supports the goal of automating the association of IT assets with network configuration management items and to enhance overall cyberspace situational awareness of physical assets, (T-1).

2.1.2.3. DELETED.

2.1.2.4. Report the loss of any IT asset with persistent storage to the ISSO, wing IA or Information Protection (IP) office, according to requirements outlined in AFI 33-200 and AFI 31-401, *Information Security Program Management*, and any local procedures.

2.1.3. **Non-Sensitive IT Assets.**

2.1.3.1. Non-Sensitive IT Assets are peripherals and other IT hardware lacking both persistent storage and IP network capabilities (e.g. mouse, keyboard, monitor, non-network displays, non-network capable Keyboard Video Mouse (KVM) switch, non-network capable fax machine, and non-network capable printer). Non-sensitive IT assets

include IT hardware providing WPAN capabilities without IP network capabilities (e.g. wireless mouse and Bluetooth keyboard).

2.1.3.2. Non-sensitive IT assets with a unit acquisition cost of $5,000 or more are accountable items and must be accounted for in AFEMS-AIM, (T-1).

2.1.3.3. Non-sensitive IT assets with a unit acquisition cost of less than $5,000 may be tracked locally IAW Material Management (23 series) policies or in AFEMS-AIM.

2.1.3.3.1. DELETED.

2.1.4. **Personal Wireless Communications System (PWCS) including Commercial Mobile Device (CMD), Cellular Phones, and Pagers.**

2.1.4.1. Any PWCS hardware meeting the definition of sensitive IT assets (persistent storage or IP network capable) must be accounted for as sensitive IT assets (e.g. CMDs, smartphones, tablets) according to **paragraph 2.1.2.2**.

2.1.4.2. If not a sensitive IT asset, PWCS hardware will be accounted for in AFEMS-AIM as PWCS commodity code "P" assets (e.g. portable radios, base stations, PWCS infrastructure equipment, Mobile Satellite Services (MSS) equipment, and Type-1 encryption capable cellular telephones).

2.1.4.3. Type-1 CMDs and Secure Mobile Environment Portable Electronic Devices (SME PEDs) will be managed by the Communications Security (COMSEC) Responsible Officer (CRO).

2.1.4.4. CMDs, cellular phones, and pagers that are not Type-1 encryption capable and do not meet the definition of sensitive IT assets are non-accountable PWCS items (e.g. basic cellular telephones and pagers).

2.1.5. **(ADDED)** Only Air Force IT assets meeting the criteria outlined in sections 2.1.2.1 and 2.1.2.2 are to be entered into, and life cycle managed, using the approved APSR.

2.1.6. **(ADDED) Accountability in the APSR**

2.1.6.1. **(ADDED)** Any asset recorded, tracked, and managed in the APSR must:

2.1.6.1.1. **(ADDED)** Adhere to the requirements described in DoDI 5000.64, Enclosure 3, Section 2.

2.1.6.1.2. **(ADDED)** Be inventoried at least annually.

2.1.6.1.3. **(ADDED)** Can only be adjusted out of the APSR with the appropriate documentation, such as disposal or transfer documentation, Accountable Property Inventory Adjustment Worksheet, DD Form 200, etc.

2.2. Hardware Assets Ordering and Procurement Guidance.

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. Quantum Enterprise Buy [QEB], Digital Printing & Imaging [DPI], Cellular Services & Devices BPAs). All AF IT hardware not purchased through AFWay, are mandated to use the NETCENTS-2 contracts, see **Chapter 4**, (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). See **Chapter 4** for details on NETCENTS-2 contracts.

2.2.1.3. Orders for equipment that will reside in SCIFs will be selected from the E/APL or other designed SCIF cognizant security authority representative prior to purchase.

2.2.1.4. DLA-Document Services is the preferred provider for printing services according to DoDI5330.03_AFI33-395.

2.2.1.5. All hardware purchases shall be in compliance with US Code Title 10 Sections 2222, 2382, and 2867, AFI 63-101, AFI 33-141, AFMAN 33-407, and the most recent published DCMO guidance for Defense Business Systems Funds Certification and Defense Business System Integrated Program/Budget Review (currently, Version 3.0 published April 2014).

2.2.2. Those submitting purchase requests will ensure a Wide Area Workflow (WAWF) Business Partner Network (BPN) number is listed at **http://www.bpn.gov/**.

2.2.3. Ensure complete information on 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.

2.2.3.1. "Mark For" information will contain; Contract Number, Purchase Order Number, Address, Phone Number, Email Address, Resource Manager Name, and Property Custodian Name (when applicable).

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

2.3. Receipt and Acceptance of 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. For IT hardware assets, the AF's official accountable property system of record is the AFEMS-AIM module or DMLSS for medical WRM assets. 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 APSR is established.

2.3.1.1.1. **(ADDED)** When received by the ECO, assets will be secured in a controlled access space (i.e. locking cabinet(s), access-controlled room/closet, segregated warehouse space, etc.)

2.3.1.1.2. **(ADDED)** When received by anyone other than the ECO, the ECO will be notified of the asset(s) delivery and the asset(s) will be secured in a controlled access

space until the asset(s) can be delivered to or picked up by the ECO. Prior ECO approval is required when deviating from the standard ECO asset(s) delivery process.

2.3.1.2. The ECO or supporting personnel will enter newly received IT assets into the APSR within 10 working days of receipt and acceptance.

2.3.1.3. **(ADDED)** Accountable IT hardware assets purchased through Government Purchase Card (GPC) must be added to the APSR and an APSR-generated Proof of Addition will be provided by the ECO to the responsible GPC holder for account reconciliation. Ensure correct MAJCOM code is entered into the APSR for all asset(s) in their DRA. The MAJCOM code must correctly identify the owning command, which may differ from the host base's command, (T-2).

2.3.1.4. For equipment not immediately installed, the ECO or supporting personnel will use the appropriate IT asset status code according to Attachment 2 (i.e., Status Code 03 - Received on-site, but not installed), (T-2).

2.3.1.5. If the receiver/acceptor of the IT asset is not the ECO or supporting personnel, the receiver/acceptor will notify the ECO upon receipt and acceptance of the IT asset so accountability is established in the AFEMS-AIM system within 10 working days of receipt and acceptance, (T-2).

2.3.1.6. 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, (T-2).

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

2.3.1.6.2. IUID labels will either be affixed to the asset by the manufacturer or will be applied by the ECO.

2.3.1.6.2.1. If the labels, placed onto the asset by the manufacturer, do not contain Cage, Part# and Serial # or if the label placed by the manufacturer does not match the data entered into AIM for the asset, then a label with the correct Cage, Part# and Serial matching the data in AIM must be placed onto the item.

2.3.1.6.3. Equivalent labels will contain the CAGE code, part number and serial number of the asset.

2.3.1.7. For holding accounts in AFEMS-AIM, the ECO login user record for holding accounts will not be used as this causes system discrepancy when trying to make changes to the DRA. The establishment of a central receiving and distribution point is mandatory for ensuring accurate accountability throughout the lifecycle of IT assets, (T-2).

2.3.2. Federal agencies must pay commercial vendor bills on time and pay interest when payments are late according to DoDFMR 7000.14-R, Volume 10, **Chapter 7**, *Prompt Payment Act*. Consequently, the AF is subject to interest penalties if the proper invoice and receiving reports for IT assets are not processed in a timely manner. To ensure timely payment to vendors and avoid interest penalties, SAF/FMP mandates the use of Wide Area Workflow (WAWF) to electronically submit all receiving reports to the Defense Finance and Accounting Service (DFAS), (T-1).

2.3.2.1. All personnel receiving or accepting IT assets on behalf of the ECO will ensure receiving reports are processed using WAWF within 3 working days of receipt and acceptance, (T-3).

2.3.2.2. If the ECO or the person who received the IT does not have visibility of the order in WAWF, the unit Resource Advisor will be contacted to ensure payment through appropriate channels, (T-3).

2.3.2.3. If WAWF is unavailable, the receiving report will be completed manually with a DD Form 250 and a copy forwarded to your local Financial Management Accounting Liaison Office (ALO) for processing to WAWF within 3 working days of IT asset receipt and acceptance, (T-3).

2.3.3. Managing Capital Assets. The Chief Financial Officers Act of 1990 (CFO Act), 31 U.S.C. §901-903, specifies capitalization and depreciation of equipment with an acquisition/leased cost equal to or greater than $100K.

2.3.3.1. Special attention needs to be taken when loading the acquisition/lease cost and the fund code. AFEMS-AIM internally computes the depreciation of these assets and reports the cost data by fund code to DFAS. The cost data for IT assets is part of the AF Financial statement that is annually submitted to Congress.

2.3.3.2. 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). The acquisition cost is typically found on an accompanying invoice.

2.4. Establishing Custodial Responsibility of Hardware Assets.

2.4.1. For effective AF hardware asset controls, custodial responsibility is established when an individual takes physical custody of the property and provides handwritten or digital signature on a custody receipt document or in a system such as an AFEMS-AIM inventory list or a hand receipt.

2.4.2. 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.

2.4.3. There are two methods to establish custodial responsibility.

2.4.3.1. Establish an organizational asset equipment account in AFEMS-AIM.

2.4.3.1.1. The organizational commander appoints a Property Custodian for the account.

2.4.3.1.2. The Property Custodian accepts custodial responsibility on behalf of the organization by certifying an AFEMS-AIM inventory list provided by the ECO with handwritten or digital signature.

2.4.3.1.3. The Property Custodian conducts the annual inventory according to paragraph 2.5.

2.4.3.1.4. Property Custodians will maintain accountability and tracking of all assigned IT assets. It is highly recommended that Property Custodian have end users sign a hand receipt or digitally sign an email or system acknowledgment for the hardware assets in the user's possession or hardware assets they use on a regular basis maintained as a KSD. Hand receipts must be accomplished for easily transported devices such as laptops, PEDs, tablets, etc. Digital signatures are encouraged, (T-2).

2.4.3.2. With prior AFECO and/or MECO approval, CSs authorize the ECO to create equipment accounts in AFEMS-AIM without assigning traditional equipment custodians. This method can only be used for smaller organizations where it is not feasible to appoint a Property Custodian. This authorization must be in writing or as a digitally signed document or email and use of hand receipts for this method is mandatory.

2.4.4. Hand receipts may be AF Form 1297, *Temporary Issue Receipt*, a digitally signed electronic hand receipt, or digital signature in an automated system. If the AF 1297 is not used, the 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." All hand receipts must be signed and contain the signer's contact information.

2.4.5. IT assets that are components of weapons systems or other major systems and are already tracked in another property management system will not be tracked in AFEMS-AIM.

2.4.6. Equipment in possession/use of deployed home station personnel will be tracked and managed within the home station inventory. Equipment transferred to other units or left forward must be properly transferred from the home station (losing unit) account to an appropriate gaining unit to maintain full accountability.

2.5. Inventory of Hardware Assets.

2.5.1. A inventory validates the existence, proper location, and correct quantity of hardware assets as stated in the inventory records in AFEMS-AIM. Inventory will be reconciled with the records contained in the AFEMS-AIM database.

2.5.2. ECOs have the authority to freeze IT asset accounts in the APSR for failure of the Property Custodian to comply with this AFMAN. This option should only be utilized after providing the Property Custodian an opportunity to correct any deficiencies in a timely manner due to the potential for serious impact to an organization's mission.

2.5.3. Official AF validation techniques for an inventory include: hands-on verification, barcode scanning, IUID, radio frequency identification (RFID), and network log-on or use records including the Enterprise IT Service Management (EITSM) suite, and using network auto-discovery tools.

2.5.4. Regardless of the validation technique used during the inventory, results of the validation will be reconciled with the records contained in the AFEMS-AIM database, (T-1).

2.5.5. The annual inventory will be conducted not later than 365 calendar days from the date the commander signed the current inventory listing. Complete out of cycle inventories when directed or required by AFECO, MECO, CSO, or ECO, (T-1).

2.5.5.1. In deployed locations, the forward commander determines the timeline for inventory based on rotation schedules.

2.5.5.2. Outgoing and incoming primary Property Custodian will conduct and certify a loss-gain joint inventory of IT assets, not later than 30 calendar days prior to being relieved of duty.

2.5.5.2.1. If the Property Custodian leaves prior to this joint loss-gain inventory being accomplished, the organizational commander assumes responsibility for all IT assets on that inventory.

2.5.5.2.2. The departing Property Custodian must reconcile missing IT assets under the guidance of the ECO prior to certifying the loss-gain inventory.

2.5.5.2.3. DELETED.

2.5.5.3. When inventory discrepancies are discovered, the Organizational Commander or Equivalent will be informed.

2.5.5.3.1. DELETED.

2.5.5.3.2. DELETED.

2.5.6. Upon completion of the IT asset inventory, the Property Custodian and the organizational commander or equivalent must approve and certify the official APSR-generated inventory with handwritten or digital signature and forwards it to the ECO, (T-2).

2.5.6.1. The commander's signature certifies to the ECO the annual inventory is complete. This date will be used as the official inventory date in AFEMS-AIM.

2.5.6.2. Annual inventories can still be certified and completed even though items are missing as long as items are documented via the Accountable Property Inventory Adjustment Worksheet or DD Form 200.

2.5.7. Only the most current IT asset inventory will be retained. (T-3).

2.5.7.1. The Property Custodian will maintain the original certified inventory and a copy will be retained in the ECO file.

2.5.7.2. If digital signatures are used, the Property Custodian and ECO will each file a copy in their electronic records management system (file plan, electronic records management solution, electronic record keeping system or automated information system).

2.5.7.3. Past inventory records and all other Key Supporting Documents (KSD) (purchase invoices, DD Form1149s, 1348s, 200s, etc.) will be kept on file for 5 years upon removal from the APSR.

2.5.7.4. The ECO, and Property Custodian will maintain electronic record folders with the following suggestions (as applicable) for each tab or directory.

2.5.7.4.1. TAB 1 – Current digitally signed Property Custodian designation.

2.5.7.4.2. TAB 2 – Current Annual Inventory.

2.5.7.4.3. TAB 3 – Hand Receipts.

2.5.7.4.4. TAB 4 – DD Form 1348-1A for disposal or disposition actions; any other disposal receipts received from DLADS.

2.5.7.4.5. TAB 5 – Asset transfer documentation.

2.5.7.4.6. TAB 6 – Training Certificates.

2.5.7.4.7. The format of the tabs will be consistent between the ECO and Property Custodian. Automated processes will be used and existing 6-part folders should be transitioned to electronic records management (e.g. AFRIMS T33-07 R07.00 as file plan baseline).

2.5.8. Property Custodians will ensure all IT assets are reflected on an AFEMS-AIM inventory listing. If hardware equipment is found in the work area that is not on the AFEMS-AIM inventory listing, determine if the equipment should be added to AFEMS-AIM to establish accountability according to guidance from the ECO and this AFMAN.

2.5.9. During the inventory, a Property Custodian will contact each individual with equipment issued via hand receipt to verify the equipment's status. At a minimum, the Property Custodian will annotate the following on his/her copy of the hand receipt: person contacted, contact date, updated contact information if required, and initial the entry. A digitally signed email, from the possessor of the equipment is the preferred method of documenting the contact, (T-3).

2.5.10. The IT asset status codes within AFEMS-AIM will be reviewed during the annual inventory to ensure the codes reflect the current status using Attachment 2, (T-2). Status codes allow the purchasing agent/entity to make accurate and informed buying decisions. For organizations that centrally procure, these codes are crucial to that process.

2.5.11. When completing inventory adjustments in AFEMS-AIM, ECOs will use the following database user's manual categories to ensure proper disposition, (T-1).

2.5.11.1. Reverse Post: A reverse post can be processed against an add asset record up and until another action has been taken against that record. Once a transaction has been processed against the record, it cannot be reverse posted.

2.5.11.2. Maintenance Swap: Assets returned to the vendor with a replacement asset provided by the vendor.

2.5.11.3. Returned: Assets returned to the Vendor without replacement.

2.5.11.4. External Disposal: This category includes assets disposed outside the normal AFEMS-AIM or Defense Logistics Agency Disposition Services (DLADS) process (e.g., transfer to organization/activities that do not use AFEMS-AIM to account for IT hardware assets).

2.5.11.5. Destroyed: This category includes Combat Losses, Natural disasters, and Authorized disposal of IT components in the area of responsibility (AOR).

2.5.11.6. Assets Tracked Elsewhere: Assets are managed on another government system.

2.5.11.7. Report of Survey: Asset has been assigned a ROS number.

2.5.12. During the inventory, AFEMS-AIM deficiencies (e.g. missing assets, incorrect locations, unrecorded property items) are identified and these deficiencies are corrected as part of the process.

2.5.13. **(ADDED) Reports of Survey (ROS)**

2.5.13.1. **(ADDED)** An ROS Investigation must be initiated:

2.5.13.1.1. **(ADDED)** For any asset being managed in the APSR that has been lost, stolen, damaged, or destroyed where the original acquisition cost is ≥ $5,000.00.

2.5.13.1.2. **(ADDED)** For any asset with an original acquisition cost < $5,000.00, but where the depreciated value at the time of the loss, theft, damage, or destruction is ≥ $500.00.

2.5.13.2. **(ADDED)** A ROS Investigation is not required when an asset managed in the APSR has been lost, stolen, damaged, or destroyed whose original acquisition cost is < $5,000.00 and has a depreciated value at the time of the loss, theft, damage, or destruction that is < $500.00.

2.5.13.3. **(ADDED)** Upon determination by the commander that an ROS Investigation is not required, the Accountable Property Inventory Adjustment Worksheet must be completed and signed before the asset can be adjusted out of the inventory. This worksheet can be found on the 38 Cyberspace Readiness Squadron's AF IT Asset Management SharePoint site at **https://cs3.eis.af.mil/sites/OO-SC-CA-45/default.aspx**.

2.5.14. **(ADDED)** For guidance on how to address a lost asset containing PII, refer to AFI 33-332, Air Force Privacy and Civil Liberties Program.

2.6. Contractor Guidance.

2.6.1. Organizational commanders grant contractor employees access to, or allow operation of, government-furnished IT resources or contractor-owned IT resources processing government information. This access is governed by the terms and conditions of the contract with the employee's company and, as appropriately coordinated with the contracting officer.

2.6.1.1. All AF-owned IT assets furnished to contractors as Government Furnished Property (GFP) will be accounted for according to this AFMAN and DoDI 5000.64, (T-1).

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

2.6.2. If contractor support employees are assigned to perform ECO duties under the terms of a contract, the AF retains responsibility for obligating funds and receiving assets as they are inherently governmental functions according to Federal Acquisition Regulation (FAR) Subpart 7.5, *Inherently Governmental Functions*.

2.6.3. Contractors may function as ITECs (if according to and within the contract provisions) for DoD-owned IT assets.

2.6.4. The Accountable Officer functions and responsibilities are defined by DoDFMR 7000.14-R, Volume 12, *Special Accounts, Funds and Programs,* **Chapter 7**. Accountable Officers exercise substantive discretionary authority in determining the U.S. Government's requirements and controlling government assets. The responsibilities of the Accountable Officer and the position of the Accountable Officer are not contractible.

2.6.4.1. Contractors may perform functions in support of the Accountable Officer and functions where they are performing according to criteria defined by the U.S. Government and allowed by the contract terms and conditions. For instance, contractors can process requisitions, maintain stock control records, perform storage and warehousing, and make local procurements of items specified as deliverables in the contract.

2.6.4.2. The administrative fund control is inherently a governmental responsibility. The contractor can process all required paperwork up to but not including funds obligation, which must be done by the government employee designated as responsible for funds control. The contractor can also process such documents as ROS and adjustments to stock levels, but approval must rest with the Accountable Officer. In all cases, the administrative control of funds must be retained by the government.

2.7. Active Duty General Officers (GO) and Senior Executive Service (SES) Civilians Notebook Computers and Portable Electronic Devices (PEDs).

2.7.1. The GO's or SES' current unit of assignment will purchase a GO and SES notebook computer/PED through the local CS (or equivalent) and follow the standard requirement process, (T-3).

2.7.2. If desired by the GO or SES, the notebook computer/PED may accompany the GO or SES from assignment to assignment. This does not include devices with a commercial wireless service contract. The GO or SES will work with the losing and gaining unit to ensure proper inventory accountability, (T-2). The local Property Custodian retains accountability for the notebook computer/PED until transferred to the new location.

2.7.3. When a GO or SES retires or leaves AF service, he or she must surrender the notebook computer/PED to the supporting ECO, (T-1).

Section 2B—Hardware Assets IT Systems Maintenance (Not Applicable to Non-AF Managed Joint Service Systems)

2.8. Support Plans. Organizations develop an Acquisitions Strategy (AS), IT asset Life Cycle Management Plan (LCMP), and/or Life Cycle Sustainment Plan (LCSP) for IT assets they procure according to AFI 63-101/20-101 to ensure logistics support throughout the expected lifecycle.

2.8.1. A support plan includes planning and developing a spare and repair parts support plan, determining initial requirements, acquisition planning, distribution, and replenishment of inventory spares. A support plan also includes periodic reviews to assure that IT assets are sustained and upgraded as necessary in accordance with the target, implementation and operational baselines according to AFPD 33-4.

2.8.2. Although there is no standard method to determine the quantity of spare equipment or repair parts to keep on hand, consider technical data such as mean time between failure rates, reliability data obtained from the manufacturer, and order and ship time from the source of supply when analyzing supply support. Personnel should also consider mission impact factors such as single point of failure and/or mission critical items. Ultimately it is the commander's or maintenance superintendent's decision based on past experience for low

density/COTS systems that determine the number of on-hand spares necessary to ensure mission accomplishment.

2.8.3. Regardless of the method used to determine the quantity of spare equipment or repair parts to keep on hand, the rationale/methodology used to determine the quantity will be documented in the AS/LCMP/LCSP.

2.8.4. Any AS/LCMP/LCSP generated by organizations outside PEO C3I&N must be coordinated with applicable MAJCOM A6, HQ AFSPC/A4C, and approved by PEO C3I&N prior to acquisition of IT hardware.

2.9. Maintenance Management. Maintenance management requirements are necessary to avoid risks to personnel, prevent damage to IT equipment, and ensure IT equipment availability to meet mission. Touch maintenance shall not be performed by personnel who are not formally task certified according to AFI 33-150, *Management of Cyberspace Support Activities,* and appropriate 3DXXX Career Field Education and Training Plan (CFETP), (T-1). This includes any action requiring removal of factory installed covers on electronic equipment for purposes other than replacement of consumables (i.e. printer toner cartridges) designed by the manufacturer as user replaceable items. This specifically includes hard drives, power supplies, internal CD/DVD drives, and circuit cards.

2.9.1. The headquarters or field-level unit determines if the IT hardware is considered mission critical or non-mission critical for maintenance management purposes.

2.9.2. Maintenance personnel performing tasks on IT hardware follow the maintenance management requirements for mission critical and non-mission critical items according to Technical Order (TO) 00-33A-1001, *General Communications Activities Management Procedures and Practice Requirements*.

2.9.3. Cannibalization may be used to satisfy an existing requirement or to meet priority mission requirements if it is the only option available to prevent mission impact. All cannibalization and documentation will be performed according to TO 00-20-3, *Maintenance Processing of Reparable Property and Repair Cycle Asset Control System*, (T-3). SCIF IT hardware assets are excluded from cannibalization actions.

2.9.4. According to TO 00-20-2, *Maintenance Data Documentation,* Chief of Maintenance/Chief of Mission Systems Flight, CS, or designated representative approval is required before any cannibalization action on mission critical IT equipment is initiated.

2.9.5. The CS Commander (or equivalent) or designated representative can approve cannibalization of operational non-mission critical IT equipment. The CS (or equivalent) must have procedures to ensure non-mission critical cannibalized IT assets are restored to full operational capability, (T-3).

2.9.6. Maintenance actions to obtain assemblies, sub-assemblies, or parts are considered transfers and are not treated as cannibalization actions. The CS (or equivalent) may retain assemblies, sub-assemblies, or parts from spare IT assets for maintenance redundancy and operational spares when the communications unit has a maintenance or operational support mission.

2.9.7. The CS Commander (or equivalent) may also approve the use of unserviceable IT hardware assets as a source for spare parts to maintain other IT equipment. This authority

should only be used when allowed by the parent MAJCOM and a cost analysis clearly determines it is economically feasible to use excess assets instead of procuring new items, (T-2).

2.9.8. Assemblies, sub-assemblies, and parts obtained for maintenance redundancy or operational spares are accounted for in the AFEMS-AIM. Ensure the IT asset status in the AFEMS-AIM is updated to identify these items as operational spares. Asset status codes are listed in Attachment 2.

2.9.9. Prior to disposition of IT assets, warranty dates must be verified to ensure items are outside their warranty expiration, (T-3).

2.10. IT Systems Maintenance Reporting. Users with maintenance contracts document all IT asset maintenance on vendor maintenance forms according to the appropriate/applicable contract. HQ AFSPC/A4/7, in coordination with HQ AFSPC/A6, will specify procedures for logging, documenting, collecting, processing, and filing copies of maintenance records according to TO 00-33A-1001.

2.11. Computation of Payments. Contracts that apply to managed hardware assets.

2.11.1. Effective Start Date for Rental or Lease. The effective date for rented/leased IT assets shall be clearly stated in the lease document – this may be a predetermined specific date or a date dependent upon the completion of specific testing and acceptance. A government-caused acceptance test delay may require payment for the delayed period. Consult the individual contract for specific guidance.

2.11.2. ECOs compute charges for rented/leased IT assets, using available vendor forms.

2.11.3. For AF-managed systems, the verifying activity refers to the equipment utilization reports and the input to the reports (IT assets/equipment orders and other appropriate records), to validate the services. Submit claims for credit within 60 calendar days (or as stated in the contract). The IT assets contract manager designates the verifying activity for non-AF managed systems (e.g., joint service systems).

Section 2C—Transfer or Disposition of Hardware Assets

2.12. Guidance for Transfer or Disposition of Hardware Assets.

2.12.1. The CS Commander (or equivalent) must ensure all assets in their DRA are cleared prior to closing that account (base closures, BRAC, mission changes, etc.). The CS (or equivalent) remains accountable for all assets until properly closed. Refer to AFI 23-111, *Management of Government Property in Possession of the Air Force*, for more specific guidance on accountable officer responsibilities. (T-1)

2.12.2. Ensure the disposition of DoD computer hard drives and/or hard drive sanitization is performed according to AFMAN 33-282. IT assets within SCIFs will follow the Intelligence Community Directive 503, Committee on National Security Systems Instruction 1253 or other policies issued by national IC elements. (T-0)

2.12.3. Software purchased with original equipment manufacturer IT is considered an integral part of the system. Therefore, the software must be maintained with the system. If the system is transferred, the software licenses must accompany the system. Transfer all

software licenses with the system. Exception may be when the terms of the software license allows for software to be recoverable and reused upon decommissioning of system assets. (T-2)

2.13. Transferring Non-excess Hardware Assets to another Department of Defense Component, Federal Agency, State, or Local Government. The transfer of non-excess IT assets occurs when a function (i.e. base realignment and closure), and the IT assets acquired to support that function, is transferred to another DoD component or Federal agency.

2.13.1. The losing Property Custodian provides the losing ECO with a letter of transfer, signed by the losing commander documenting the transfer of the function and equipment.

2.13.2. Ensure a DD Form 1149, Requisition and Invoice/Shipping Document, is signed and dated by a designated official from the shipping activity (Traffic Management Office or commercial carrier) and the Property Custodian. For local transfers where no shipping activity is involved, the gaining and losing Property Custodian signs the DD Form 1149.

2.13.3. The losing activity ECO will account for the transferred hardware. The ECO will also identify excess hardware created as a result of the transfer of a function.

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

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

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

2.13.4. The losing ECO will:

2.13.4.1. Update the asset status field in AFEMS-AIM using the codes in Attachment 2.

2.13.4.2. Provide account records information to the gaining activity as required.

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

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

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

2.13.4.6. Ensure hard drive sanitization according to AFMAN 33-282.

2.13.4.7. Provide the hardware system database records or custodian report to the Property Custodian. The Property Custodian will add all applicable records regarding the transfer to their applicable electronic records.

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

2.13.4.9. Notify the AFEMS Help Desk to delete or archive the records of the equipment being transferred.

2.14. Excess Hardware. An item is considered excess when it is no longer required due to mission change, equipment upgrades, technology changes, obsolescence, etc. The item is also considered excess when the total quantity on hand exceeds the required quantity, as identified in the technical solution/requirements document, plus the number of authorized spares as identified in the AS/LCMP/LCSP. According to AFI 23-111, accountable individuals are responsible for properly identifying, reporting, and determining correct disposition of unserviceable, reparable, or excess property.

2.14.1. MECOs or base CSs/ECOs, when permitted by their MECO, may develop their own excess hardware assets retention policies. However, the rationale for the retention policy must be approved by Air Force Life Cycle Management Center (AFLCMC) and documented in the AS/LCMP/LCSP.

2.14.2. The ECO will authorize the Property Custodian to retain serviceable excess asset items for maintenance redundancy or operational spares if allowed by the parent MAJCOM.

2.14.3. The Property Custodian will notify the ECO when hardware assets become excess NLT 30 calendar days before the equipment goes off line if possible. This allows completion of the screening cycle while the equipment is still in use, eliminating the need to store excess assets. If not possible, until receipt of final disposition instructions, the Property Custodian will store the equipment to prevent damage, deterioration, or unauthorized cannibalization.

2.14.4. Available AF excess assets can be located using DLADS at **http://www.dispositionservices.dla.mil/**. ECOs must use the AFEMS-AIM module to process any excess IT assets in AIM. Other methods or systems (DLADS Electronic Turn-in Documents [ETIDS]) may be used for non-sensitive IT assets not tracked in AIM.

2.14.5. Dispose of and/or reuse classified media and systems according to remanence security guidance in AFMAN 33-282.

2.15. Obtaining Excess Resources.

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

2.15.2. To acquire equipment from DLADS, the Property Custodian submits documentation (DD Form 1348-1A) for coordination to the ECO. Assets can either be viewed at the DLADS location or researched at **http://www.dispositionservices.dla.mil/**.

2.15.3. ECOs establish accountability in the AFEMS-AIM for hardware equipment acquired through any source that meets the criteria for accountability in accordance with this AFMAN.

2.16. Transferring Excess Hardware Assets to the DLADS.

2.16.1. DLADS is the primary DoD agent for disposal of all obsolete, unserviceable, or excess military property and equipment. All AF hardware will be disposed of through the DLADS.

2.16.2. DLADS guidelines for excess and the disposal of hardware assets can be found at **http://www.dispositionservices.dla.mil/**.

2.16.3. All media being disposed of or transferred to DLADS or another entity outside of the DoD will be sanitized and/or destroyed as applicable according to AFMAN 33-282.

2.16.4. ECOs must establish an MOA with their servicing DLADS office in order to transfer IT equipment directly to local schools under the Computers for Learning Program. Donations of IT equipment to schools can only take place after completion of the mandatory DoD reutilization screening and then the IT equipment may be donated only to registered and qualified institutions identified by the DLADS.

2.16.5. No IT assets can be donated directly to a school or other government entity without the approval of the DLADS.

2.16.6. ECOs will use AIM generated 1348A to process DLADS disposals. ETIDS will not be used for these transactions.

2.17. Exchange or Sale of Government Automated Resources.

2.17.1. Contract partners have programs designed to recover (give credit for equipment that still has market value) and recycle (dispose of hardware assets in an environmentally safe manner and replace due to obsolescence or un-serviceability) hardware assets. The proceeds or credit is applied toward the purchase of replacement government automation resources. See DoD 4140.1-R, *DoD Supply Chain Materiel Management Regulation* and *Defense Federal Acquisition Regulation Supplement (DFARS)*, current edition, Part 217.70, *Exchange of Personal Property*, for more specific guidance.

2.17.2. Adherence to disposal procedures in NIAP PPs or DoD STIGs is required. When those resources are unavailable or do not address disposal, following remanence security requirements according to AFMAN 33-282 is vital to all transactions relating to excess IT including warranty exchanges.

Chapter 3

SOFTWARE ASSET MANAGEMENT

3.1. Software Assets General Guidance and Procedures. Software asset management shall be centralized and managed at the highest level of common usage but no lower than the BSLM, (T-2). The CS Commander (or equivalent) at each installation implements licensed COTS or other software for local requirements not fulfilled by enterprise software licensing. The management of software licenses at the base level does not include those software licenses that are managed through enterprise software licensing programs. Software asset management program ensures organizations that deploy and manage COTS software track software entitlements and implementation information.

3.1.1. Organizations will maintain a hard or soft copy of the software license inventory and "Proof-of-License Ownership" of GOTS/COTS software in use within their organization.

3.1.2. Organizations will store proof of license agreements or licenses (e.g. user manuals, purchase documentation, CDs, etc.) and software media in a secure centralized location (e.g., locked drawer, file cabinet, room, etc.) or electronically if applicable. Work with local Functional Area Record Manager or Base Records Management Office to ensure proper retention and disposition of official records and records approval in the office file system.

3.1.3. Organizations will inventory all licensed software annually and, if available utilize auto-discovery tools, to track and report implemented software and license information. The Organization commander will certify the annual inventory with a handwritten or digital signature indicating completion of the inventory and submit to the BSLM (or equivalents).

3.1.4. Organizations will audit all systems to ensure no illegal or unauthorized copies of software is installed. Sampling procedures may be used if active inventorying/auto discovery systems are available.

3.1.5. Automated tools should be used to the maximum extent possible for tracking software installed on the base network where applicable. Note: AFEMS-AIM should not to be used for tracking software licenses.

3.1.6. All implemented software must be certified for use according to AFI 33-210 and free of viruses and malicious logic.

3.1.7. All common-user desktop/laptop software on new computer systems will comply with the AF SDC.

3.1.8. The BSLM will annually instruct organizations and personnel on appropriate licensed software usage considering *The Copyright Act*, E.O. 13103, *Computer Software Piracy*, this AFMAN and applicable DoD guidance, (T-3).

3.1.8.1. Coordinate instruction through the local JA office to ensure accuracy in the message before instructing how, and to what extent, a user may be held liable for unauthorized or illegal use of computer software.

3.1.8.2. Place semi-annual reminders of the need for proper software license management in base bulletins and other media to increase and reinforce the legal requirement of maintaining software licenses according to their stated conditions.

3.1.9. DELETED.

3.1.10. DELETED.

3.1.11. Redistribute excess or superseded software if it:

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

3.1.11.2. Is not classified.

3.1.11.3. Did not provide direct security protection to systems that processed classified information.

3.1.11.4. Is not directly related to or associated with a weapon system, intelligence system, command and control system, communications system, or tactical system.

3.1.11.5. Still operates as intended.

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

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

3.1.12.2. Destroy the software and license keys according to the provisions of the licensing agreement. Document the method of destruction to establish an audit trail.

3.2. Ordering and/or Procuring Software.

3.2.1. All AF software will be procured using applicable AF enterprise buying programs (T-1).

3.2.1.1. AF Enterprise License Agreements (ELAs), Joint or DoD ELAs authorized for AF use, and DoD ESI/SmartBuy, are the primary source for software purchased, (T-1).

3.2.1.1.1. For information on available AF, Joint or DoD ELAs, contact SAF/CIO A6 Capabilities Division.

3.2.1.1.2. DoD Enterprise Software Initiative (DoD ESI): **http://www.esi.mil/**.

3.2.1.2. Any COTS product, maintenance, and related hardware or services not offered by an ELA or DoD ESI must be procured using an approved contract vehicle such as NETCENTS-2, GSA IT Schedule 70, or NASA SEWP, (T-1). See **Chapter 4** for details on and approved contract vehicles.

3.2.2. All software for use on Air Force networks must be evaluated and certified/assessed by the appropriate Security Control Assessor (SCA), formerly known as the Certification Authority according to AFI 33-210, (T-1). The list of evaluated products can be found at **https://cs1.eis.af.mil/sites/AFCKS/Compliance/Lists/Approved_Software/AllItems.aspx**.

3.2.3. All requests for server software must comply with current National Defense Authorization Act as depicted in AFI 33-150. A DOD Unique identifying number must accompany the acquisition.

3.2.4. All software purchases shall be in compliance with US Code Title 10 Sections 2222, 2382, and 2867, AFI 63-101, AFI 33-141, AFMAN 33-407, and the most recent published

DCMO guidance for Defense Business Systems Funds Certification and Defense Business System Integrated Program/Budget Review (currently, Version 3.0 published April 2014).

3.3. Software Developed Using Commercial Off-The-Shelf (COTS) Office Software Tools. Personnel are required to use licensed COTS office software to increase productivity and overall organization effectiveness. Users must obtain approval from the CS (or equivalent) before developing shared single-user, networked multi-user, or "group" computer applications built with COTS office software tools. This precludes later impact on network and server capacity, avoids duplication of effort on similar application software within the installation or MAJCOM, and ensures continued software support after departure of one or more of the original user-developers, (T-1). AF user-developers shall:

3.3.1. Ensure the AF retains property rights to the computer software developed in the course of their duties, (T-1).

3.3.2. Not bypass computer and network server operating systems, security systems, or access controls provided by higher authority, (T-1).

3.3.3. Provide the CS Commander (or equivalent) a software documentation package in appropriate digital format, (T-2). The software package must include:

3.3.3.1. The author or point of contact, organization, and telephone number.

3.3.3.2. A descriptive unclassified title with version number as the first delivery (use Version 1.0).

3.3.3.3. A brief (one paragraph) unclassified description of the software's functionality for use in publishing software catalogs; and a classified description, if necessary, to more fully explain the software's capabilities.

3.3.3.4. A brief description of all testing performed on the mission application software and its databases.

3.3.3.5. A brief user's guide. The user's guide should include:

3.3.3.5.1. The hardware configuration required.

3.3.3.5.2. The supporting software required including the operating system and any supporting COTS software with version release number.

3.3.3.5.3. Compiling and linking instructions, if applicable.

3.3.3.5.4. Descriptions of the software installation process, required hardware setup, menus, and software capabilities and functions.

3.3.3.5.5. Samples of output screens and print products produced (if any).

3.3.3.5.6. Other information useful for continued effective use and maintenance of the mission application software.

3.4. Command, Control, Communications, Computers, and Intelligence (C4I) Software Development, Reuse, and Release. Adhere to DoDD 4630.05, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*; DoDI 4630.8, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems*; and Chairman Joint Chiefs of Staff Instruction (CJCSI) 6212.01E,

Interoperability and Supportability of Information Technology and National Security Systems when developing mission or application software for C4I systems.

3.4.1. Do not develop software organically unless quality, cost, performance, schedule, or interoperability requirements cannot be met with COTS or non-developmental item software. Develop requirements for IT capabilities in accordance with AFPD 10-6, *Capabilities-Based Planning & Requirements Development*. This applies to AF Program Objective Memorandum (AFPOM)-funded units.

3.4.1.1. Acquire an approved mission needs statement before developing organic software requiring over 6 man-months of effort or costing in excess of $50,000. If software is developed organically through a contractor, the contract must contain the proper FAR/DFAR clauses on data rights.

3.4.1.2. All units that develop or maintain software will have a software process improvement (SPI) program and a documented SPI plan, including at least:

3.4.1.2.1. A baseline of their current capabilities.

3.4.1.2.2. Goals and milestones they intend to reach.

3.4.1.2.3. Metrics to measure their progress toward their goals and milestones.

3.4.1.2.4. Timeline for SPI appraisals. The Software Technology Support Center (STSC) at Hill Air Force Base, Utah is available on a fee-recovery basis for SPI appraisals, but any qualified SPI appraiser may be used.

3.4.1.2.5. Identify life-cycle support requirements for the life of developed software.

3.4.2. Government Software Release or Disclosure. It is AF policy to release, upon consideration of a valid written request, specific software developed with government funds, which is a government work (created by government personnel) or software created by a contractor where the AF has a government rights license. Release of software by the AF is not permitted if it violates a copyright or terms of a contract. The OPR for the software is the approval authority to release or disclose that software. Additional approval may be required at a higher level depending upon the recipient in accordance with AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program*. When not for foreign release and the OPR is in doubt regarding the release of software, send the request to SAF/CIO A6 for resolution. Freedom of Information Act (FOIA) requests must be sent to the local FOIA manager to control and respond using guidelines in the AF supplement to DoD 5400.7-R_AFMAN 33-302 (DoD 5400.7-R), *Freedom of Information Act Program*.

3.4.2.1. Before releasing the software, the OPR shall require the requester to sign a MOA. The MOA shall be written to govern maintenance and support relationships for the software or document the lack of these relationships if the OPR will not provide support.

3.4.2.2. Releases of AF-owned or developed software from software reuse libraries, or software under AF-industry Cooperative Research and Development Agreements (CRADA), are exceptions to this policy.

3.4.3. When developing mission or application software for information systems, it is desirable to utilize the Software Engineering Institute's Software Capability Maturity Model

Integrated (CMMI) as advised by the STSC (http://www.stsc.hill.af.mil), or the Systems Engineering Process (SEP), maintained by the Program Executive Office for Business and Enterprise Systems (AFPEO BES) (http://public.gunter.af.mil/applications/sep/menus/Main.aspx).

3.5. Software Configuration, Change, and Release Management. Use AF IT Services Methods and Procedures Technical Orders (MPTOs) for Configuration Management and Change Management as applicable. Use ISO/IEC 20000, or Information Technology Infrastructure Library (ITIL), Configuration Management, Change Management, and Release Management processes to plan, identify, control, monitor, verify, and manage software configuration items. Typically, software configuration items would include information such as purchase order number, purchase date, software manufacturer, software title, and version implemented.

3.5.1. AF Form 2519, *All Purpose Checklist*, will be used for software and software license management as needed.

3.5.2. Program managers and software developers must integrate information assurance into their systems using guidance contained in AFPD 33-2 and the AF 33-200 series publications. These publications give policy guidelines for developing and using the computer, communications, and emissions security programs needed for all AF communications and information systems.

3.5.3. The AF is committed to meeting the DoD objective of developing interoperable and maintainable systems based on open standards. DoD and AF guidance identifies a common set of mandatory IT standards and guidelines used in all new systems and system upgrades in the DoD. To that end, system developers, contract administrators, and maintainers must:

3.5.3.1. Adhere to the guidance given in the DoD Information Enterprise Architecture (DoDIEA).

3.5.3.2. Adhere to the guidance given in the target, implementation, and operational baselines according to AFPD 33-4.

3.5.3.3. Each unit ensures that upgrades to systems under maintenance comply to the maximum extent possible with the DoDIEA and AF baselines as they are updated.

3.5.4. The AF is committed to sharing AF information to those with a validated need for the information. To that end, it is important that architectural artifacts capture the roles and permissions of users of AF information, in context of the supported mission and business processes, and that authorization and access to AF information is provisioned to support the defined roles and permissions.

3.5.5. Software reuse is the practice of using existing software components to develop new software applications. Software reuse benefits the AF through increased developer productivity, improved quality and reliability of software-intensive systems, enhanced system interoperability, lowered program technical risk, and shortened software development and maintenance time.

3.5.5.1. Reusable software components may include executable software binaries, source code segments, program documentation, project plans, requirement descriptions, design and architecture documents, database schemas, test data and test plans, user's manuals, software tools, and object classes.

3.5.5.1.1. These assets are most efficiently reused when designed to fit into a product-line architecture for a mission area or functional domain using standard interfaces and common communications protocols.

3.5.5.1.2. Domain product-line components can be used to create families of related systems designed to share a common software architecture for the domain.

3.5.5.2. The AF Integration Test Lifecycle Capability maintains a software reuse library or repository for internal sharing of the reusable software components developed at the location.

3.5.6. The AF is faced with restrictions on the amount of information that can be provided to our forces, particularly in remote areas of the world. Therefore, software designers and developers must discipline themselves in the quantity and content of non-mission essential information sent over supporting network infrastructures (that is, ensuring sending only operationally necessary data).

3.5.6.1. In addition to DoD direction, follow all policy and procedures in AFMAN 33-152, *User Responsibilities and Guidance of Information Systems* on downloading from the Internet, transmission of email attachments, video teleconferencing, Web browsing, and conservation measures during periods of surge or network degradation.

3.5.6.2. AF-developed software (including that developed specifically for the AF) will accommodate network infrastructure considerations into its systems design and internal code, such that it does not overtax the infrastructure on which it relies and operates.

3.5.7. The AF will develop new software capabilities only as a last resort if no other solutions satisfy requirements. When developing software, focus should be on web-centric application development without dependence on specific client platforms so that the end-user device can be agnostic to the mission application: Unless technically or operationally unfeasible, all services developed or procured will comply with the following key elements:

3.5.7.1. Be based on bounded user requirements with all information assets described through detailed business process re-engineering and generating Quality of Service (QoS), performance, and access rules consistent with associated architecture products, support plans and Service Level Agreements (SLAs).

3.5.7.2. Be web-enabled with data made visible, discoverable, and accessible using open, standard, lightweight protocols and techniques.

3.5.7.3. Be clientless with all web services and applications accessible securely via standard web browsers from AF-standard desktops or other edge devices.

3.5.7.4. Utilize strong two-way authentication using public key infrastructure (PKI) when available.

Chapter 4

NETCENTS-2

4.1. The NETCENTS-2 contracts enable delivery of products, services and solutions that adhere to the AF Enterprise Architecture (AF EA).

4.1.1. The suite of NETCENTS-2 contracts will provide Netcentric Products, NetOps and Infrastructure Solutions, Application Services, IT Professional Support and Engineering Services (Advisory & Assistance Services (A&AS), and Enterprise Integration and Service Management (A&AS). **http://www.netcents.af.mil/contracts/netcents-2/index.asp**.

4.1.2. After each of these categories is awarded, the NETCENTS-2 contracts will be available through the AFWAY portal at **https://www.afway.af.mil/**.

4.2. The NETCENTS-2 contracts will be the primary source used by AF customers to support missions that require voice, data, and video communications, information services, solutions, and products. All new and ongoing Air Force acquisition efforts shall incorporate NETCENTS-2 into their acquisition strategy according to AFI 63-101. Programs already in the 8(a) program will remain in the 8(a) program until removed by Small Business according to FAR 19.203(c).

4.3. Contracting officers work with the NETCENTS Program Management Office (PMO) to determine if a requirement for a proposed IT acquisition falls outside the scope of NETCENTS-2 contracts. All IT requirements shall be coordinated with the appropriate functional level (i.e., the CS (or equivalent) at base level, A6 at MAJCOM level) prior to submittal for contract action.

4.4. NETCENTS-2 contracts will follow the fiscal guidance in AFI 65-601V1 and DOD Financial Management Regulation Volume 2A to determine thresholds for investment funding and proper appropriations for IT resources.

MICHAEL J. BASLA, Lt Gen, USAF
Chief, Information Dominance
and Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

E.O. 13103, *Computer Software Piracy,* 30 September 1998

The Copyright Act of 1976

The Chief Financial Officers (CFO) Act of 1990, 31 U.S.C. §§901-903

CJCSI 6212.01E, *Interoperability and Supportability of Information Technology and National Security Systems*, 15 December 2008

FAR, Subpart 7.5, *Inherently Governmental Functions*, FAC 2005-13, 19 May 2006

DFARS, Subpart 217.70, *Exchange of Personal Property,* 21 June 2005

DoDFMR 7000.14-R, Volume 1, **Chapter 3**, *Federal Financial Management Improvement Act of 1996 Compliance, Evaluation, and Reporting,* October 2008

DoDFMR 7000.14-R, Volume 10, **Chapter 7**, *Prompt Payment Act*, December 2009

DoDFMR 7000.14-R, Volume 12, *Special Accounts, Funds and Programs*, 30 August 2011

DoD 4140.1-R, *DoD Supply Chain Materiel Management Regulation*, 23 May 2003

DoD 5400.7-R_AFMAN 33-302, *Freedom of Information Act Program*, 21 October 2010

DoDD 4630.05, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 5 May 2004

DoDD 8000.01, *Management of the Department of Defense Information Enterprise*, 10 February 2009

DoDD 8320.02, *Data Sharing In A Net-Centric Department of Defense*, 2 December 2004

DoDI 4630.8, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 30 June 2004

DoDI 5000.64, *Accountability and Management of DoD Equipment and Other Accountable Property*, 19 May 2011

DoDI 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information*, 9 October 2008

DoDI 8500.2, *Information Assurance (IA) Implementation*, 6 February 2003

ISO/IEC 19770, *Software Asset Management (SAM)*

ISO/IEC 20000, *Information Technology - Service Management*

AFPD 10-6, *Capabilities-Based Planning & Requirements Development*, 31 May 2006

AFPD 33-1, *Information Resources Management*, 27 June 2006

AFPD 33-2, *Information Assurance (IA) Program*, 3 August 2011

AFPD 63-1/20-1, *Integrated Life Cycle Management*, 3 July 2012

AFPD 65-2, *Managers' Internal Control Program*, 28 August 2006

AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program,* 1 December 2004

AFI 23-111, *Management of Government Property in Possession of the Air Force,* 7 January 2011

AFI 31-401, *Information Security Program Management*, 1 November 2005

AFI 31-501, *Personnel Security Program Management*, 27 January 2005

AFI 33-129, *Web Management and Internet Use*, 3 February 2005

AFI 33-150, *Management of Cyberspace Support Activities*, 30 November 2011

AFI 33-200, *Information Assurance (IA) Management,* 23 December 2008

AFI 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP),* 23 December 2008

AFI 33-590, *Radio Management,* 8 April 2013

AFI 38-101, *Air Force Organization*, 16 March 2011

AFI 63-101/20-101, *Integrated Life Cycle Management,* 7 March 2013

AFI 90-201, *The Air Force Inspection System*, 23 March 2012

AFMAN 23-220, *Reports of Survey for Air Force Property*, 1 July 1996

AFMAN 33-152, *User Responsibilities and Guidance for Information Systems,* 1 June 2012

AFMAN 33-282, *Computer Security (COMPUSEC),* 27 Mar 2012

AFMAN 33-363, *Management of Records,* 1 March 2008

OMB Circular A-130, *Management of Federal Information Resources,* 28 November 2000

T.O. 00-20-2, *Maintenance Data Documentation*, 1 September 2010

T.O. 00-20-3, *Maintenance Processing of Reparable Property and Repair Cycle Asset Control System*, 1 November 2008

T.O. 00-33A-1001, *General Communications Activities Management Procedures and Practice Requirements,* 1 December 2012

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 Publications*

AF IMT 2519, *All Purpose Checklist*

AF Form 1297, *Temporary Issue Receipt.*

Abbreviations and Acronyms

ACES-RP—Automated Civil Engineers System-Real Property

AETC—Air Education and Training Command

AF—Air Force

AFECO—Air Force Equipment Control Officer

AFEMS—Air Force Equipment Management System

AFI—Air Force Instruction

AFLCMC—Air Force Life Cycle Management Center

AFMAN—Air Force Manual

AFMC—Air Force Materiel Command

AFMOA—Air Force Medical Operations Agency

AFPD—Air Force Policy Directive

AFPEO BES—Air Force Program Executive Office for Business and Enterprise Systems

AFR—Air Force Reserve

AFPSC—Air Force Space Command

AFWay—Air Force Way

AIM—Asset Inventory Management

ALO—Accounting Liaison Office

ANG—Air National Guard

AOR—Area of Responsibility

AS—Acquisitions Strategy

BPN—Business Partner Network

BRAC—Base Realignment and Closure

BSLM—Base Software License Manager

C&A—Certification and Accreditation

C4—Command, Control, Communications, and Computers

C4I—Command, Control, Communications, Computers, and Intelligence

CAGE—Commercial and Government Entity code

CFETP—Career Field Education and Training Plan

CFL—Computers for Learning

CIO—Chief Information Officer

CJCSI—Chairman Joint Chiefs of Staff Instruction

CMD—Commercial Mobile Device

CMDB—Configuration Management Database

CMMI—Capability maturity Model Integrated

CO—Contracting Officer

COMPUSEC—Computer Security

COMSEC—Communications Security

COTS—Commercial Off-the-Shelf

CRADA—Cooperative Research and Development Agreements

CRO—Communications Security (COMSEC) Responsible Officer

CS—Communications Squadron

CST—Client System Technician

CYRS—Cyber Readiness Squadron

CtO—Certificate to Operate

DD—Department of Defense (used on forms only)

DFARS—Department of Defense Federal Acquisition Regulation Supplement

DFAS—Defense Finance and Accounting Service

DLADS—Defense Logistics Agency Disposition Services

DoD—Department of Defense

DoDAAC—DoD Activity Address Code

DoDD—Department of Defense Directive

DoDFMR—Department of Defense Financial Management Regulation

DoDI—Department of Defense Instruction

DoDIEA—DoD Information Enterprise Architecture

DMLSS—Defense Medical Logistics Standard Support

DRA—Defense Reporting Activity

DRU—Direct Reporting Unit

E/APL—Evaluated/Approved Products Listing

ECO—Equipment Control Officer

ELA—Enterprise License Agreement

EITSM—Enterprise IT Service Management

E.O—Executive Order

ESI—Enterprise Software Initiative

ETIDS—Electronic Turn-in Document

FAR—Federal Acquisition Regulation

FOA—Field Operating Agency

FOB—Found-On-Base

FOIA—Freedom of Information Act

GFP—Government Furnished Property

GO—General Officer

GOTS—Government Off-The-Shelf Software

HTSA—Host Tenant Support Agreement

HQ—Headquarters

IA—Information Assurance

IAW—In accordance with

IC—Intelligence Community

IP—Internet Protocol

IT—Information Technology

ITAM—Information Technology (IT) Asset Management

ITEC—Information Technology Equipment Custodian

ITIL—Information Technology Infrastructure Library

ISO/IEC—International Standardization Organization/International Electrotechnical Commission

IUID—Item Unique Identification

KVM—Keyboard Video Mouse

LCMP—Life Cycle Management Plan

LCSP—Life Cycle Sustainment Plan

MAJCOM—Major Command

MECO—Major Command Equipment Control Officer

MICT—Management Internal Control Toolset

MOA—Memorandum of Agreement

MPTO—Methods and Procedures Technical Order

MSO—Managed Services Office

MSS—Mobile Satellite Services

NETCENTS—Network-Centric Solutions

NIAP PP—National Information Assurance Partnership Protection Profiles

NLT—No Later Than

NSA—National Security Agency

NSS—National Security System

OPR—Office of Primary Responsibility

PEC—Personal Wireless Communications System Equipment Custodian

PED—Portable Electronic Device

PEO C3I&N—Program Executive Office for Command Control Communications Infrastructure and Networks

PKI—Public Key Infrastructure

PMO—Program Management Office

PWCS—Personal Wireless Communications Systems

QoS—Quality of Service

RDS—Records Disposition Schedule

RFID—Radio Frequency Identification

RFQ—Request for Quotation

ROS—Report of Survey

SAF—Secretary of the Air Force

SAP—Special Access Program

SAM—Software Asset Management

SCI—Sensitive Compartmental Information

SCIF—Sensitive Compartmental Information Facilities

SDC—Standard Desktop Configuration

SEP—Systems Engineering Process

SES—Senior Executive Service

SIM—Serialized Item Management

SLA—Service level Agreement

SME-PED—Secure Mobile Environment Portable Electronic Device

SPI—Software Process Improvement

STIG—Security Technical Implementation Guide

STSC—Software Technology Support Center

TO—Technical Order

USAF—United States Air Force

UTC—Unit Task Code

WAWF—Wide Area Workflow

WPAN—Wireless Personal Area Network

WRM—War Reserve Material

Terms

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.

AutoDiscovery Tool—Applications that can audit computers and services for physical and software configuration information.

Business Partner Network (BPN)—The equivalent to DoDAACs and are the critical data link in identifying the responsible organization to accomplish a WAWF receiving report.

Cannibalization—Authorized removal of a specific assembly, subassembly or part from one system for installation on another end item to satisfy an existing supply requisition and to meet priority mission requirements with an obligation to replace the removed item. Canning is the act of removing serviceable parts from one IT system for installation in another IT system when removal of parts will cause the first system to not perform as designed.

Client Support Technician (CST)—CSTs support customers with resolving issues relating to information technology devices, such as personal computers, personal digital assistants, and printers. (AFMAN 33-152)

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 Mobile Device (CMD)—A subset of portable electronic devices (PED) as defined in DoDD 8100.02 that provide one or more commercial wireless interfaces along with a compact user input interface (Touch Screen, Miniature Keyboard, etc.) and exclude PEDs running a multi-user operating system (Windows OS, Mac OS, etc.). This definition includes, but is not limited to smart phones, tablets, and e-readers.

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.

Communications Equipment—All communications systems and equipment including but not limited to ground-based radio and wireless systems including infrared; radar, meteorological and navigational radiation aids used for aircraft control and landing; radiating aids for fire control; imagery, video processing equipment and intrusion detection systems, satellite, microwave and telemetry equipment; mission critical computer hardware, telecommunications switching equipment, cable and antenna systems; cryptographic equipment and communications consoles; and electronic counter-measures and related radiation, re-radiation, and electronic devices.

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.

Configuration Management Database (CMDB)—A CMDB is a database that contains all relevant information about the components of the information system used in an organization's IT services and the relationships between those components. Typically includes hardware, software, and topology information.

Department of Defense (DoD) Redistribution Program—Worldwide program, initiated by DoD for reporting, screening, redistributing, and disposing of automation resources that have become excess under an original application.

Designated Approving Authority (DAA)—The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority. (DoDI 8500.2)

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.

Enterprise License—Allows the purchasing organization to use multiple copies of a specific 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 Control Officer (ECO)—An individual appointed by the applicable CS to manage and control IT assets resources for a base. (**Note:** A tenant unit may have its own ECO. This should be coordinated among the main base Communications unit, the tenant unit, and the MAJCOM of the tenant unit.)

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

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.

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)

Information Technology Equipment Custodian (ITEC)—An individual who acts as a subordinate to the applicable ECO and performs inventory, utilization, and maintenance recording and reporting and other custodial duties as the ECO requires.

Interoperability—The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. The condition achieved among communications-electronics systems or items of communications-electronics equipment when exchanging information or services directly and satisfactorily between them and/or their users.

Joint Service System—A standard system implemented at one or more services sites (U.S. Army, U.S. Navy, U.S. Air Force, and U.S. Marine Corps). Systems acquisition, development, maintenance, and life-cycle support are assigned to a program manager assigned to one of the services.

KSD—Key Supporting Documentation

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 A6 that oversees the management and control of IT assets for the MAJCOM, FOA, and DRU

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.

Peripheral—Any equipment that provides the IT system with additional capabilities distinct from the central processing unit (e.g., a printer, mouse, disk drive, digitizer, etc.).

Pilferable—Items having a ready resale value, civilian utility or application, and therefore are especially subject to theft. Consideration must be given to the cost to provide controlled storage and handling compared to the potential losses when selecting items to be treated as pilferable items. Generally an item should not be coded for worldwide treatment as pilferable, unless the unit cost exceeds $100 and repetitive losses indicate the item is subject to theft; however, the unit cost criteria may be waived when management determines that losses on an item warrant the cost of additional controls.

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.

Resources—Any IT system, component hardware and software, contractual services, personnel, supplies, and funds.

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

Sensitive Information—The loss, misuse, unauthorized access to, or modification of information that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C. Section 522a (*The Privacy Act*), but that has not been specifically authorized under criteria established by an E.O. or an Act of Congress to be kept SECRET in the interest of the national defense or foreign policy.

Shareware—Privately or commercially developed software that users receive free of charge but pay a fee for continued or extended use. Normally, implied or promised support by the author is minimal or nonexistent.

Software—(1) A set of 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.

Systems Administrator—The organization focal point for multi-user systems

User—The individual who operates the computer or uses application software.

Attachment 2

EQUIPMENT STATUS REPORTING

A2.1. The AFEMS-AIM status codes in Table A2.1. describe the operational status of a component or DRA. Valid values are:

Table A2.1. IT asset status codes for equipment status reporting.

Status Code	Status Description
01	Programmed, planned, or unapproved order.
02	Approved acquisition, or on order.
03	Received on-site, but not installed.
04	Undergoing acceptance testing, during installation.
11	Installed, accepted, and in use.
12	Available excess.
41	Discontinued use.
52	Transferred in from another DRA.