

**BY ORDER OF THE
SECRETARY OF THE AIR FORCE**



AIR FORCE INSTRUCTION 33-112

7 JANUARY 2011

688 IOW SUPPLEMENT

24 JANUARY 2012

Communications and Information

**INFORMATION TECHNOLOGY
HARDWARE ASSET MANAGEMENT**

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/A6NT

Certified by: SAF/A6N (Col Kaufman)

Pages: 39

Supersedes: AFI33-112, 7 April 2006

(688IOW)

OPR: 23 IOS/OSF

Certified by: 688 IOW/DS (Ms. Laura L. Hawkins)

Pages: 6

Supersedes: AFI33-112_688IOWSUP_1,
1 May 2010

This Air Force instruction (AFI) implements Air Force Policy Directives (AFPD) 33-1, *Information Resource Management*; AFPD 33-2, *Information Assurance (IA) Program*; AFPD 20-1, *Acquisition and Sustainment Life Cycle Management*; and AFPD 10-6, *Capabilities Base Planning & Requirements Development*, by identifying responsibilities for supporting Air Force information technology equipment (computer systems). One or more paragraphs of this AFI do not apply to non-Air Force-managed joint service systems. These paragraphs are marked as follows: *(NOT APPLICABLE TO NON-AIR FORCE-MANAGED JOINT SERVICE SYSTEMS)*. Refer technical questions about this AFI to Air Force Network Integration Center (AFNIC/ESPL), 203 West Losey Street, Room 1200, Scott AFB IL 62225-5222. 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 disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at <https://www.my.af.mil/afrims/afrims/afrims/rims.cfm>. Submit policy and procedural recommendations for Information Technology (IT) asset management to AFNIC/ESPL. Send recommended changes or comments to AFNIC/EASD, 203 West Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using Air Force (AF) Form 847,

Recommendation for Change of Publication, with an information copy to the Office of the Secretary of the Air Force for Warfighting Integration and Chief Information Officer, Director of Information, Director, Network Services (SAF/A6N), 1250 Air Force Pentagon, Washington DC 20330-1250. 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.

(688IOW) AFI 33-112, *Information Technology Hardware Asset Management*, is supplemented as follows: This instruction assigns responsibilities and provides procedures related to managing information technology equipment. It clarifies and further defines responsibilities and procedures established in AFI 33-112, *Information Technology Hardware Asset Management*, 7 January 2011. This instruction applies to all 688th Information Operations Wing (688 IOW) Commanders/Directors, Information Technology Equipment Custodians (ITECs), Information Assurance Officers and Client Support Administrators assigned to Lackland Air Force Base, TX. All geographically separated units (GSUs) will follow their associated Base Equipment Control Officer (ECO) office guidelines and supplements to AFI 33-112. This publication does not apply to Air Force Reserve Command nor Air National Guard units. Refer recommended changes and questions about this instruction to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 through the appropriate functional's chain of command. Ensure that all records created as a result of processes prescribed in this memorandum are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at <https://www.my.af.mil/gcss-af61a/afirms/afirms/>.

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed. The main focus is to clarify roles and responsibilities. Paragraph 3 added responsibilities of AF/A2. Paragraph 4 is changed to define new roles for AFNIC. Paragraph 6 is changed to replace HQ OSSG/LRE with 754 Electronic Systems Group. Paragraph 7 removes responsibility from Communications and Information Systems Officer (CSO) for labeling IT assets. Paragraph 8 changes clarify Organization Commander responsibilities and replaces Air Force Systems Security Instruction (AFSSI) 5020 reference with AFSSI 8580. Paragraph 9 clarifies that AFNIC will perform MAJCOM Equipment Control Officer (MECO) duties as part of the MAJCOM A6 workload consolidation effort. Paragraph 10 changed to allow for digital signatures in lieu of wet signatures. Paragraph 10 clarified definition of annual for the purpose of conducting annual inventories. Paragraph 10 also changed to allow for the development of local forms. Paragraph 11 changed the name Equipment Custodian to IT Equipment Custodian (ITEC) and clarified ITEC responsibilities. Paragraph 13 changed to clarify Air Force Contractor responsibilities associated with government furnished equipment. Paragraph 14 changed to remove items covered in other instructions. Paragraph 17 changed to clarify IT shipping requirements. Paragraph 18 was added to address receipt and acceptance of IT assets. Paragraph 19 added to address establishing custodial responsibility. Paragraph 20 added to address physical inventory and also addresses the use of automated network tools to assist with IT asset inventory. Paragraph 21 changed to reflect change in publication from AFSSI 5020 to AFSSI 8580.

Paragraph 22 added to clarify capital asset reporting. Paragraph 23 changed to reflect a change in reference material. Paragraph 26 changed to clarify procedures for turning in excess equipment. Paragraph 29 added to address exchange or sale of government automated resources. Paragraph 30 changed to reflect an update to the records disposition rule. Attachment 2 changed to reflect changes in the core document.

(688IOW) This document is substantially revised and must be completely reviewed. This supplement was updated to align with new terminology, requirements, and schedules associated with the newly released core reference, AFI 33-112, dated 7 Jan 2011.

Section A—Responsibilities	4
1. Directorate of Network Services (SAF/A6N).	4
2. Director, Security, Counterintelligence and Special Program Oversight (SAF/AAZ).	4
3. Deputy Chief of Staff, Intelligence, Surveillance, and Reconnaissance, (AF/A2).	5
4. Air Force Network Integration Center (AFNIC).	5
5. Headquarters Air Education and Training Command (HQ AETC/A3T).	6
6. Electronic Systems Command (ESC/HGGG).	6
7. Communications and Information Systems Officers (CSO):	7
8. Organization Commanders or Equivalent.	8
9. Major Command Equipment Control Officers.	10
10. Equipment Control Officers (ECO).	10
11. Information Technology Equipment Custodians (ITEC).	12
Section B—General Guidance and Procedures	14
12. Network and Computer Security.	15
13. Air Force Contractor Employees.	15
14. Acquisition of Information Technology (IT) Assets.	15
15. Active Duty General Officers (GO) and Senior Executive Service (SES) Civilians Notebook Computers and Personal Digital Assistants (PDA).	16
16. Environmental Considerations .	17
Section C—Inventory, Accountability, Transfer, and Reporting of Information Technology (IT) Systems (Note: Consult AFI 33-115, Volume 1, Network Operations (NETOPS), for additional guidance in determining the types and quantities of equipment needed to support the network).	17
17. Inventory Management and Accountability of IT Hardware Assets.	17
18. Receipt and Acceptance of Information Technology Assets	18
19. Establishing Custodial Responsibility.	19

20.	Physical Inventory of IT Hardware Assets.	20
21.	Transferring Non-excess Information Technology (IT) Assets to another Department of Defense Component, Federal Agency, State, or Local Government.	20
22.	Managing Capital Assets	21
Section D—Information Technology (IT) Systems Maintenance (Not Applicable to Non-Air Force Managed Joint Service Systems)		22
23.	Support Plans.	22
24.	Information Technology (IT) Systems Maintenance Reporting.	23
25.	Computation of Payments.	23
Section E—Disposition of Excess Information Technology (IT) Resources		23
26.	Excess.	23
27.	Obtaining Excess Resources.	24
28.	Transferring Excess Information Technology (IT) Systems Assets to the DLA Disposition Services (formerly DRMO).	24
29.	Exchange or Sale of Government Automated Resources.	25
30.	Information Collections, Records, and Forms.	25
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		27
Attachment 2—INFORMATION TECHNOLOGY (IT) SYSTEMS CHECKLIST		35
Attachment 3—EQUIPMENT STATUS REPORTING		39

Section A—Responsibilities

1. Directorate of Network Services (SAF/A6N).

- 1.1. Develops, publishes, and disseminates Air Force doctrine and policy for IT asset systems.
- 1.2. Identifies formal IT management training requirements.
- 1.3. Works in conjunction with Defense Logistics Agency Disposition Services (formerly DRMO) on disposition of excess IT assets.

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

- 2.1. Is appointed as the Air Force Director of the Special Access Program (SAP) Central Office. The Director is responsible for establishing, developing, coordinating and implementing SAP policies and procedures for general oversight, execution, management, administration, security, information assurance and maintenance of records for all SAPs for which the Air Force has responsibility and will ensure compliance through guidelines, inspections, regulations and other measures.

2.1.1. SAP information technology assets under the cognizance of the Director, SAF/AAZ, will be tracked in the Assets Inventory Management (AIM) module of the AF Equipment Management System (AFEMS), and hereafter noted as AFEMS-AIM, on a case by case basis. The Director will evaluate all security issues and concerns before rendering a determination as to which assets will be tracked. The Director will provide this determination in writing. IT assets which cannot be tracked using the AFEMS-AIM will be separately tracked within the SAP enterprise.

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

3.1. In accordance with DoDD 8520.1 and AFPD 33-2, 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 authorities granted by the Director of National Intelligence, relevant national Intelligence Community (IC) elements, and DoD, AF/A2 may delegate specific duties, roles, and responsibilities for providing policy and oversight for IT assets residing in SCIFs, are components of AF SCI systems, or make up national-level intelligence, surveillance and reconnaissance systems.

3.2. Air Force information technology assets under the cognizance of AF/A2 will be tracked in AFEMS-AIM or, when available, the Expeditionary Combat Support System (ECSS) if the cognizant security authority representative determines that there are no security concerns. AF/A2 or designated representative will provide guidance for meeting regulatory compliance for IT assets not tracked in AFEMS-AIM or ECSS.

4. Air Force Network Integration Center (AFNIC).

4.1. Provides guidance and support to MAJCOMs, field operating agencies (FOA), and direct reporting units (DRU) in developing, integrating, implementing, and managing IT assets.

4.2. Reviews, evaluates, and interprets issues/problems and makes recommendations to SAF/A6NT on policy changes.

4.3. Reviews, interprets, and disseminates Air Force policy.

4.4. Acts as office of primary responsibilities (OPR) for this instruction.

4.5. Acts as functional manager for the IT component of AFEMS-AIM. Provide guidance on transferring IT component management from AFEMS-AIM to ECSS.

4.6. Resolves management issues on IT hardware assets accounted for in the AFEMS-AIM module and resolves policy disagreements between MAJCOMs, functional managers, and non-Air Force agencies.

4.7. Perform MECO responsibilities described in this AFI as required under the terms of memoranda of agreements executed with the MAJCOMs in the course of transfer of A6 workload responsibilities.

4.8. Establishes and chairs the Air Force Computer Systems Management (CSM) Working Group (CSMWG) to directly support CSM personnel at all levels including MAJCOM Equipment Control Officers (MECO), Communications and Information Systems Officers (CSO), Equipment Control Officers (ECO), organizational commanders and Information

Technology Equipment Custodians (ITEC) in the execution of their responsibilities as delineated in this instruction. The CSMWG provides broad representation allowing for improved cross feed of information and feedback from the field necessary to make informed decisions about CSM policy and procedures. The CSMWG serves as the Air Force CSM management infrastructure to deal with all CSM-related issues in an efficient and effective manner.

4.8.1. The CSMWG will:

- 4.8.1.1. Develop proposed solutions on issues affecting IT system life-cycle management.
- 4.8.1.2. Identify functional improvement opportunities for review, prioritizing, approval, and budgeting considerations.
- 4.8.1.3. Advise Air Force leadership on IT management issues.
- 4.8.1.4. Define new functional requirements and provide oversight to automated information systems (AIS) processes supporting Air Force IT management.
- 4.8.1.5. Work with the IT Commodity Council on procurement initiatives.
- 4.8.1.6. Work with AF/A2 appointed representative on SCIF issues.

5. Headquarters Air Education and Training Command (HQ AETC/A3T).

5.1. Provide formal IT training to support responsibilities of AF Chief of Staff in training AF personnel. SAF/A6N will provide direction regarding AETC delivered IT training.

6. Electronic Systems Command (ESC/HGGG).

- 6.1. Functions as Program Manager for the AFEMS-AIM module.
- 6.2. Submits the special year-end chief financial officer report to the Defense Finance and Accounting Service (DFAS).
- 6.3. Proposes technical solutions for defined requirements.
- 6.4. Coordinates all requirements and associated cost data through the program agreement (PA) manager for review and approval.
- 6.5. Notifies the PA manager of all unfunded requirements.
- 6.6. Coordinates software releases through the PA manager prior to scheduled release. Refer to AFPD 33-2, para.5.7, requirement to secure AFNETOPS/CC (DAA) certification and approval prior to release.
- 6.7. Provides input to program management reviews.
- 6.8. Completes Life Cycle Management Plan (LCMP) and Information Support Plan/certification documentation. (see AFI 63-101, *Acquisition and Sustainment Life Cycle Management*).
- 6.9. Develops and maintains the AFEMS-AIM User's Manual on the AFEMS Community of Practice at <https://wwwd.my.af.mil/afknprod/ASPs/CoP/OpenDMCop.asp?Filter=OO-LG-MC-46>.
- 6.10. Provides operations, programming, and software support.

7. Communications and Information Systems Officers (CSO):

7.1. Process all base-user computer systems orders except those excluded by host tenant support agreements and joint service programs managed outside the Air Force. Orders for equipment that will reside in SCIFs will be approved by the SCIF System Security Officer (SSO) or other designed SCIF cognizant security authority representative prior to purchase.

7.2. Are the accountable officer for all IT hardware equipment listed in their assigned Defense Reporting Activity (DRA). Ensures the AFEMS-AIM inventory is used to provide accountability of all base IT hardware resources assigned to that DRA. Refer to paragraph 17 to determine if a particular piece of IT hardware equipment should be accounted for using methods or systems other than AFEMS-AIM.

7.3. Assist in planning and execution of all activities related to the deployment of systems.

7.4. Assist the supporting contracting officers in developing an acquisition strategy for maintenance contracts.

7.4.1. Follow budgeting arrangements established in host tenant support agreements.

7.5. Analyze IT asset maintenance cost data to assist in developing cost-effective maintenance solutions. IT assets within SCIFs are excluded.

7.5.1. Direct retention of serviceable excess IT assets, when allowed by the parent MAJCOM, for maintenance redundancy or operational spares, by ensuring use of sharing and redistribution programs to meet user requirements.

7.5.2. Authorize removal/transfer of unserviceable IT assets for spare parts.

7.5.3. Authorize cannibalization of IT assets to satisfy critical mission requirements. Maintenance actions to obtain assemblies, subassemblies, or parts from spare IT assets are considered transfers and will not be treated as cannibalization actions.

7.6. Authorize cannibalization of unserviceable computer systems for spare parts. IT assets within SCIFs are excluded.

7.7. Coordinate action to ensure secure, climate controlled, and easily accessible facilities with sufficient floor space are provided to the ECO for receiving, storing, and distributing IT assets. The establishment of a central receiving and distribution point is highly encouraged for ensuring accurate accountability throughout the lifecycle of IT assets.

7.8. Coordinate on IT asset requirements with the appropriate office or unit.

7.9. Appoint, in writing, a minimum of one primary and one alternate ECO and provides a copy of the appointment letter to the MECO. Digital signatures may be used in lieu of wet signatures. Although no grade restrictions apply for these positions, the primary and alternate ECOs should have the leadership skills and IT asset knowledge necessary to provide guidance and direction to the ITEC. The recommended minimum rank/grade requirement for the primary ECO is Technical Sergeant/GS-7. An airman (Senior Airman or below) may be appointed as an alternate ECO, if the CSO believes the airman is mature enough to handle the responsibility. See paragraph 13 for contractors. **Note:** The primary ECO will supervise the alternate ECO in performance of duties and responsibilities.

7.10. Direct the use of Hand Receipts (i.e. AF Form 1297) as necessary to maintain span of control.

8. Organization 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.

8.1. Budget for maintenance of computer systems that are not the responsibility of the CSO.

8.2. Review and coordinate on organization's requirement documents.

8.3. Submit unit computer systems requirements to the applicable CSO for technical solutions according to AFI 33-103, *Requirements Development and Processing*.

8.4. Review assigned IT assets annually to determine if the IT is obsolete, still meets user requirements or needs modification and acts accordingly.

8.5. Appoint, in writing, a minimum of one primary and one alternate ITEC, no later than 45 calendar days prior to the projected departure of the current ITEC. ITECs may be military (see note) or civilians. Contractors may also be ITECs in support of the accountable officer according to AFI 23-111, *Management of Government Property in Possession of the Air Force*, under the specific terms of the contract and must be mutually agreeable to the organization commander and the CSO. This applies to active duty, guard, and reserve personnel. Foreign nationals or local wage rate employees (foreign nationals in host countries) may be appointed primary or alternate custodians only when they may be held pecuniary liable for losses of equipment under the law of the host country. Organization commanders must review the provisions and restrictions outlined in AFI 31-501, *Personnel Security Program Management*, AFI 33-200, *Information Assurance (IA) Management*, and AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program*, before appointing foreign nationals as primary or alternate equipment custodians. **Note:** An airman (Senior Airman or below) may be appointed primary or alternate custodian by the organization commander, if the commander believes the airman is mature enough to handle the responsibility.

8.5.1. Forward the ITEC appointment letter and request for ITEC training to the ECO.

8.5.1.1. The ITEC appointment letter must be dated and must contain the names and signatures of the primary and alternate ITECs. Digital signatures may be used in lieu of wet signatures.

8.5.1.2. Ensure the primary or alternate ITEC is scheduled for training with the ECO within 30 calendar days of initial appointment and annually thereafter.

8.5.1.3. Annually review ITEC appointment letters and training dates to ensure the primary and alternate ITEC names are current and they have completed annual ITEC training. If the primary or alternate ITEC has changed, forward a new ITEC appointment letter as described in paragraph 8.5.1.1 to the ECO. When possible, the review should be held in conjunction with the annual inventory.

8.5.2. Require departing ITECs to process out through the ECO.

8.5.3. Ensure outgoing primary and incoming primary ITEC conduct and sign a loss-gain joint physical inventory. The departing ITEC must reconcile missing items under the guidance of the ECO, not later than 30 calendar days prior to the primary ITEC being relieved of duty. In deployed locations, the forward commander will determine timeline for transfer of duties based on rotation schedules.

8.5.3.1. Refer to AFMAN 23-220, *Reports of Survey for Air Force Property*, to process a Report of Survey (ROS) when there are inventory discrepancies that cannot be resolved prior to the custodian's departure. An ROS is mandatory to adjust accountable records.

8.5.4. **(Added-688IOW)** If the primary ITEC is deployed for a period exceeding 120 days, a new ITEC should be appointed in writing prior to the deployment. If replaced, the departing Primary and gaining ITECs must complete a Loss/Gain inventory prior to the Primary ITEC departing.

8.6. Ensure the ITEC perform a complete and accurate annual inventory. After the annual inventory is complete, the commander or equivalent signs the inventory listing. Digital signatures may be used in lieu of wet signatures. The commander's signature certifies to the ECO that the annual physical inventory is complete. The annual inventory will be conducted not later than 365 calendar days from the date the commander signed the most current inventory listing.

8.7. Ensure the ITEC notify the applicable ECO of any computer systems that are scheduled for deployment.

8.8. Promote user awareness concerning unauthorized or illegal use of computer systems hardware and software.

8.9. Ensure all AFEMS-AIM accountable IT assets are reported to the ECO for inclusion in the AFEMS-AIM inventory.

8.10. Ensure that the applicable ECO coordinates on the "Ship To" addressee on all purchase requests or transfers that involve computer systems.

8.11. Ensure the disposition of Department of Defense (DoD) computer hard drives and/or hard drive sanitization is performed in accordance with the procedures outlined in Air Force Systems Security Instruction (AFSSI) 8580, *Remanence Security*. IT assets within SCIFs will follow the Joint DoDIIS /Cryptologic SCI Information Systems Security Standards or other policies issued by national IC elements.

8.12. **(Added-688IOW)** Coordinate with the ECO to establish enough ITE accounts to effectively manage the organization's ITE assets.

8.12.1. **(Added-688IOW)** Establish accounts using organizational or geographical considerations. Accounts should not be spread over several different offices/rooms/buildings. ITECs must be able to maintain positive control over the equipment in their accounts.

8.12.2. **(Added-688IOW)** Accounts should contain an appropriate number of assets that allow for effective tracking by the ITEC. It is recommended that each ITEC be responsible for no more than 500 ITE assets.

9. Major Command Equipment Control Officers.

9.1. The MAJCOM CSO or FOA/DRU equivalent appoints, in writing, the MECO unless MECO duties were assumed by AFNIC as part of the MAJCOM A6 workload consolidation effort. AFNIC/CC appoints the MECO for those that have transferred MECO duties. Although no grade restrictions apply for this position, the MECO should have the depth and experience necessary to provide guidance and direction to the ECO. Recommend minimum grade be a senior non-commissioned officer (SNCO)/GS-9 for this position. When the MECO changes, the MAJCOM CSO notifies AFNIC/ESPL (afnic.espl.it@us.af.mil) by electronic mail (e-mail), so their official listings can be updated with the new name, office symbol, phone number, and e-mail address. The MECO will:

- 9.1.1. Provide guidance and procedural policy to the ECOs on management of IT hardware assets.
- 9.1.2. Work with other MECOs to determine reporting procedures of tenant units and continue to work together to resolve any problems that might arise.
- 9.1.3. Approve or reject transfer of IT assets between losing and gaining commands.
- 9.1.4. Send applicable ECO concerns about the inclusion and/or exclusion of IT hardware assets in AFEMS-AIM to AFNIC/ESPL, 203 West Losey, Room 1200, Scott AFB, IL 62225-5222 , through e-mail to afnic.espl.it@us.af.mil, or via phone to DSN 779-6280.
- 9.1.5. Review finalized excess reports completed by applicable ECOs and ensure appropriate action is accomplished.
- 9.1.6. Allow ECOs to create and maintain holding accounts for known near-term requirements.
- 9.1.7. Provide assistance for the establishment of a new DRA and IT data system connectivity, as required.
 - 9.1.7.1. Maintain a copy of the ECO's appointment letter. The MECO forwards the AFEMS-AIM Access Request to the program management office (PMO) for action and retention.
- 9.1.8. Provide assistance to applicable ECOs in closing out a DRA (e.g., base closures).
- 9.1.9. Disseminate information provided by HQ USAF, HQ AFNIC, and PMO to applicable ECOs.
- 9.1.10. Establish accountability for IT assets acquired through joint services PMs, as required.
- 9.1.11. Approve or reject requests to turn in or reutilize IT assets outside of their DRA.

10. Equipment Control Officers (ECO).

10.1. The CSO appoints the primary and alternate ECO according to paragraph 7.9. See paragraph 13 for contractors. Due in part to guidelines in DoD *Financial Management Regulation*, Volume 1, Chapter 3 and AFPD 65-2, *Managers' Internal Control Program*, the ECO cannot be the ITEC for any AFEMS-AIM account other than an account established for holding assets prior to distribution or disposal (i.e. holding or excess accounts). If holding

accounts are used, normal account management requirements still apply (i.e. appointment letters, 365 calendar day inventory frequency, etc.).

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

10.2. The ECO, or ECO designated receiving official, will receive all AFEMS-AIM accountable IT assets, complete necessary documentation according to paragraph 18 and determine the method used to account for IT according to paragraph 19.3.

10.2.1. If the IT hardware is accounted for in AFEMS-AIM, ensure the IT asset status code in AFEMS-AIM is updated using the codes identified in Attachment 3. Review the IT asset status codes during the annual inventory to ensure the codes reflect the current status.

10.2.2. The ECO is responsible for equipment listed in his/her assigned DRA.

10.2.3. Assist the ITEC in determining the ownership of all Found-On-Base (FOB) IT assets.

10.2.4. Direct ITECs to conduct, at a minimum, a complete annual inventory of all IT assets assigned to the ITEC's AFEMS-AIM account and ensure the inventory is completed. Review ITEC appointment letters annually to ensure the primary, alternate ITEC and appointing authority names are current and they have completed annual ITEC training. The review of ITEC appointment letters should be held in conjunction with the annual inventory. The annual inventory will be conducted not later than 365 calendar days from the date the commander signed the most current inventory listing. The date the commander signs the inventory will be used to update the AFEMS-AIM last inventory date.

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

10.2.4.2. ECOs have the authority to lock ITEC accounts for failure to comply. This option should only be utilized after providing the ITEC an opportunity to correct any deficiencies in a timely manner due to the potential for serious impact to an organization's mission.

10.2.5. Authorize the ITEC to retain serviceable excess IT asset items for maintenance redundancy or operational spares when allowed by the parent MAJCOM.

10.2.6. Retain unserviceable excess IT asset hardware for cannibalization as directed by the CSO.

10.2.7. Ensure correct MAJCOM code is entered into AFEMS-AIM for all IT assets in their DRA. The MAJCOM code must correctly identify the owning command which may differ from the host base's command.

10.2.8. Provide the ITEC with AFEMS-AIM generated or equivalent labels.

10.2.9. Work with the ITEC to update the inventory as dictated by a ROS. Use of the Department of Defense (DD) Form 200, *Financial Liability Investigation of Property Loss*, to adjust accountable records is mandatory.

10.2.10. Complete out-processing for departing ITEC upon transfer of account and receipt of new appointment letters and signed joint loss-gain inventory.

10.2.11. Provide guidance and annual training for the ITEC. Annual training must be documented in AFEMS-AIM. Upon request, the ECO provides their commanders with documentation verifying names of the ITECs trained, material covered, and training dates.

10.2.12. Take guidance and direction from the MECO and CSO.

10.2.13. Deploy AFEMS-AIM accountable, UTC tasked IT assets at the request of the ITEC or deployment authority. AFEMS-AIM will be used to accomplish the deployment.

10.2.14. Establish accountability for IT hardware assets acquired through joint services, working with the parent MAJCOM.

10.2.15. Attempt to reutilize excess organizational IT assets that meet minimum network configuration standards before offering equipment to organizations outside the DRA, when allowed by the parent MAJCOM.

10.2.16. After receipt of a transportation fund site, direct the losing custodian to prepare the necessary shipping documents for items that are excess and required by other services.

10.2.17. Coordinate with any tenant ECO to establish a host tenant agreement identifying any assistance required, such as AFEMS-AIM connectivity.

10.2.18. Coordinate on all host-tenant support agreements (HTSA) concerning IT asset management. IT accountability support can be specified in the HTSA or a Memorandum of Agreement (MOA).

10.2.19. May develop and mandate use of locally generated products and/or forms to ensure accurate documentation and data entry for the addition, transfer, deletion, or disposal of IT assets.

10.2.20. (**Added-688IOW**) The ECO will conduct a Staff Assistance Visit (SAV) on every account at least once each calendar year. Also, the ECO may conduct random SAVs throughout the year, or as requested by the ITEC or commander.

11. Information Technology Equipment Custodians (ITEC).

11.1. Accountable for all assigned IT hardware assets in their account and will:

11.1.1. Perform, at a minimum, an annual physical inventory of all items in the AFEMS-AIM account. Also, conduct additional inventories when directed by the ECO. Upon completion of the inventory, the ITEC and the organizational commander or equivalent must sign the inventory. The original will be retained by the ITEC and a copy will be retained in the ECO file. If digital signatures are used, the ITEC 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). The annual inventory will be conducted not later than 365 calendar days from the date the commander signed the most current inventory listing.

- 11.1.1.1. During the inventory, ensure all assets can be traced back to an AFEMS-AIM inventory listing. If IT hardware equipment is found in the work area that is not on the AFEMS-AIM inventory listing, refer to paragraph 17 to determine if the IT equipment should be added to AFEMS-AIM to establish accountability IAW guidance from the ECO.
- 11.1.1.2. During the annual physical inventory, an ITEC will contact the individual to whom the equipment is issued via hand receipt to verify the equipment's status. At a minimum, the ITEC will annotate the following on the hand receipt; person contacted, date of contact, and ITEC initials.
- 11.1.2. Only the most current inventory must be retained in the ITEC/ECO folder or Electronic Records Management system. Additional inventories may be retained as deemed necessary for historical purposes. Review past inventory records before disposing of old inventory data and ensure source documents are retained to support current inventory records, e.g., Reports of Survey, hand receipts, etc. Recommend using 6-part folders or electronic records management system.
- 11.1.3. **(Added-688IOW)** Ensure, as a minimum, that all Accountable-Method Optional ITE assets (a current list of accountable assets is posted and maintained on the Air Force Portal under the Air Force tab and the Enterprise IT Initiatives heading) are accounted for using the 688 IOW ITEC Equipment Database or equivalent. The minimum information required to be tracked is make, model, serial number, part number, description, purchase date, cost, and location. The ITEC will maintain a copy of the spreadsheet in the ITEC continuity folder.
- 11.2. Ensure all accountable IT assets, excluding devices that are too small, have AFEMS-AIM generated or equivalent labels affixed. When the device is too small, user generated labels including CAGE, part number, and serial number may be used.
- 11.3. Obtain approval and coordinate all potential transfers of IT assets between ITEC accounts with the applicable ECO where practical.
- 11.4. Report all FOB IT assets to the applicable ECO and accept accountability or distribute equipment as directed by that ECO.
- 11.5. Sign for new equipment received through the ECO.
- 11.6. Take guidance from the ECO on all shipments (incoming and outgoing), transfers, donations, or turns-ins of excess IT assets.
- 11.7. Provide appropriate documentation to the applicable ECO to clear the account of 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 (formerly DRMO).
- 11.8. Remain responsive to applicable ECO.
- 11.9. Must out-process through the applicable ECO.
- 11.10. Conduct a joint physical inventory (outgoing primary ITEC with incoming primary ITEC) and reconcile any missing items, via ROS or hand receipt, before permanent change of station, permanent change of assignment, separation, or retirement (minimum of 30 calendar

days prior). Incoming ITEC will contact the individual to whom the equipment was issued to verify the equipment's status.

11.11. Initiate the ROS process according to AFMAN 23-220, concerning any lost, damaged, or destroyed IT assets.

11.11.1. **(Added-688IOW)** The ITEC will staff a ROS initiation request through their organizational chain to the ECO explaining extent of search

11.11.2. **(Added-688IOW)** The ECO will forward to the 688 IOW CSO for approval/disapproval. The CSO will then forward approved requests to the 688 IOW Report of Survey (ROS) Monitor. Disapproved requests are returned to initiator with further instructions.

11.11.3. **(Added-688IOW)** ROS' for Geographical Separated Units (GSUs) are processed through their host base ECO office vice the Wing ECO office. GSUs will follow host base procedures for completing ROS'.

11.12. Notify the applicable ECO of excess IT assets.

11.13. Provide the applicable ECO a serialized numbered list of any AFEMS-AIM accountable UTC tasked assets that will deploy.

11.14. Receive and secure all IT assets, if not received by the ECO, until proper accountability is established.

11.14.1. **(Added-688IOW)** Ensure all ITE assets are properly accounted for by submitting the required letters to the ECO. Once properly accounted for, the ITEC must check with the unit IAO to ensure the equipment has been added to the proper system security package (SSP) before being put into use. Guidance is provided in AFI 33-101, *Communications and Information Management Guidance and Responsibilities*; the *Joint DoDIIS\Cryptologic SCI Information Systems Security Standards (JDCSISSS)*; and DoD Regulation 5200.40, *DoD Information Technology Security Certifications and Accreditation Process*.

11.15. Coordinate with Information Systems Security Officer (ISSO) to ensure the ISSO sanitizes hard drives according to the procedures outlined in AFSSI 8580.

11.16. **(Added-688IOW)** The ITEC will conduct a self-inspection semi-annually (January/July) using the ECO-provided self-inspection checklist. Maintain the self-inspections in the ITEC continuity folder until their next SAV has been completed. Results are due to the ECO by the 20th of the month it is conducted.

11.16.1. **(Added-688IOW)** For any discrepancies noted, the ITEC will provide the results, fix actions, and timeline to the ECO. The ECO will monitor fix actions identified by the ITEC.

11.17. **(Added-688IOW)** Note that all duties apply equally to both primary and alternate ITECs.

Section B—General Guidance and Procedures

12. Network and Computer Security. Refer to AFI 33-200 *Information Assurance (IA) Management*.

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

13.1. Contractors may function as ITECs (if so stipulated in the contract) for DoD-owned IT assets as the contract specifies.

13.2. DoDI 5000.64, *Accountability and Management of DoD-Owned Equipment and Other Accountable Property*, requires DoD Components to establish records and maintain accountability for property (of any value) furnished to contractors as Government Furnished Property (GFP).

13.2.1. All Air Force owned IT furnished to contractors as GFP will be accounted for according to paragraph 17 in this instruction.

13.3. Establish the extent of contractor liability in the provisions of the applicable contract's government property clause. (See AFI 23-111 *Management of Government Property in Possession of the Air Force*.)

13.4. If contractor support employees are assigned to perform ECO duties under the terms of a contract, the Air Force retains responsibility for obligating funds and receiving assets as they are inherently governmental functions. (See FAR 7.5, *Inherently Governmental Functions*)

13.5. The functions and responsibilities of the Accountable Officer are defined by DoD 7000.14-R, Volume 12, *Special Accounts, Funds and Programs*, August 2009. 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.

13.6. Contractors can perform functions in support of the Accountable Officer and functions where they are performing in accordance with criteria defined by the U.S. Government. 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.

13.7. The responsibility for administrative fund control is inherently governmental. The contractor can process all required paperwork up to 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 stockage levels, but approval must rest with the Accountable Officer. In all cases, the administrative control of funds must be retained by the government.

14. Acquisition of Information Technology (IT) Assets.

14.1. Procurement through the AF Information Technology Commodity Council (ITCC) buying programs is mandatory for all IT product categories encompassed by those programs, such as the Quantum Enterprise Buy (QEB) for desktop and laptop computers unless waived

by the MAJCOM CIO/A6 or as noted in 14.1.1 below. Products offered through the ITCC buying programs are available exclusively through AFWay (<https://www.afway.af.mil>).

14.1.1. Defense Logistics Agency Document Services, *formerly DAPS*, is the preferred provider to meet requirements for high volume, large copy count and large page count, high speed copying services and production. Air Force units are not required to purchase or lease DPI equipment from DLA Document Services unless the DLA Document Services solution is clearly a better value. For complete information on DLA Document Services refer to <http://www.daps.dla.mil/index.html>

14.1.2. Even if the ITCC buying strategy has been waived, the use of AFWay is still mandatory unless waived by the MAJCOM CIO/A6 for the purchase of all IT products under the purview of the ITCC as listed in 14.1 above. For products not listed in the AFWay catalogue, purchasers may use the request for quote (RFQ) feature to get pricing for their unique requirements.

14.2. NETCENTS contracts, upon award, are the mandatory source for purchasing netcentric and information technology products and solutions that fall under the scope of those contracts but outside the scope of ITCC managed products as discussed in 16.1. Deviation from this mandate requires written approval from the appropriate governance body, depending on the dollar value and risk level of the acquisition. Detailed governance, processing, and purchasing information is available on the NETCENTS portal, which is also accessible through AFWay (<https://www.afway.af.mil>).

14.3. Process all base user IT purchases as prescribed above except those excluded by host tenant support agreements and Joint Service programs managed outside the Air Force.

14.4. Air Force organizations purchasing common use IT assets (i.e. non-mission system assets) for NIPR or SIPR in AF SCIFs are directed to use AFWAY and NETCENTS unless AF/A2, a designated AF/A2 representative, or a SCIF cognizant security authority representative determines there is a security or information assurance concern. When purchasing SCIF NIPR or SIPR IT assets is through alternate procurement vehicle(s) (outside of AFWAY or NETCENTS), the asset will comply with, or exceed, the established asset capability and interoperability standards set by the Air Force Information Technology Commodity Council, Air Force Network Integration Center, or 24th Air Force. Organizations should not purchase IT components that violate SCIF operating standards (i.e., components that emit or record emissions) even when the components are SIPR or NIPR baseline capabilities. When purchasing information technology assets for use on TS networks, the use of AFWAY and NETCENTS is encouraged when the procurement vehicle satisfies cost, information assurance, and operational security concerns.

15. Active Duty General Officers (GO) and Senior Executive Service (SES) Civilians Notebook Computers and Personal Digital Assistants (PDA).

15.1. Active Duty GO and SES personnel, including brigadier general selects and SES Civilian appointees, are required to maintain e-mail contact with the Chief of Staff of the Air Force. The GO's or SES' current unit of assignment will purchase a GO and SES notebook computer/PDA through the local communications unit and follow the standard requirement process. If desired by the GO or SES, the notebook computer/PDA may accompany the GO or SES from assignment to assignment. If GOs or SES' decide to take their notebook

computer/PDA, they will work with the losing and gaining communications unit to ensure proper inventory accountability. The local ITEC retains accountability for the notebook computer/PDA until transferred to the new location.

15.1.1. When a GO or SES retires or leaves Air Force service; he or she must turn in the notebook computer/PDA to the supporting ECO.

16. Environmental Considerations . Use hardware and software within the environmental parameters defined by the vendor (e.g., power, temperature, humidity, etc.).

16.1. Equipment damage outside these parameters may void the warranty or incur an added cost liability according to the contract constraints.

16.2. Commanders may authorize use outside the environmental parameters if mission requirements dictate (e.g., deployed operations).

Section C—Inventory, Accountability, Transfer, and Reporting of Information Technology (IT) Systems (Note: Consult AFI 33-115, Volume 1, Network Operations (NETOPS), for additional guidance in determining the types and quantities of equipment needed to support the network).

17. Inventory Management and Accountability of IT Hardware Assets.

17.1. Guidance for determining the accountability of IT assets is governed by multiple and complex congressional, federal, DoD, and Air Force policies. In order to simplify the determination of Air Force accountable IT assets, a comprehensive and current list of accountable assets is posted and maintained on the Air Force Portal (<https://www.my.af.mil>) under the Air Force tab and the Enterprise IT Initiatives heading.

17.1.1. Management and oversight of the official Air Force accountability list is the responsibility of the CSMWG.

17.2. Ensure complete information on shipping labels. 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 IT equipment.

17.2.1. –Mark For” information will contain; Contract Number, Purchase Order Number, Address, Phone Number, e-mail Address, Resource Manager Name, and ITEC Name (when applicable).

17.2.2. –Ship To” information will contain the complete delivery address. This includes the Equipment Control Officer name. This will correspond to the DoD Activity Addressing Codes (DoDAAC) and the system of record for real property (ACES-RP).

17.3. 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, software and system documentation must accompany the system. Transfer all documentation with the system.

17.4. Software license management is explained in AFI 33-114, *Software Management*.

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

17.6. Equipment that is deployed and remains in possession/use of home station personnel who are deployed should be tracked and managed within the home station inventory. Equipment that is 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.

17.7. **(Added-688IOW)** Accountability of ITE and other computer equipment is the joint responsibility of unit commanders and division chiefs, the 688 IOW ECO, appointed ITECs, CSTs, and each individual user. Accountability is the obligation imposed by law, lawful order, or regulation on an officer or other persons for keeping accurate records of property, documents, or funds. Accountability is concerned primarily with records while individual responsibility is primarily concerned with custodianship, care, and safekeeping.

17.7.1. **(Added-688IOW)** To ensure personal accountability and responsibility within the 688 IOW, each user will be required to complete the Individual Responsibilities and Personal Accountability training (via Plateau) at least once every 365 days.

17.7.2. **(Added-688IOW)** For Accountable-Method Optional ITE assets, accountability is the responsibility of the organizational commander with the following exceptions:

17.7.2.1. **(Added-688IOW)** 688 IOW requires all monitors to be tracked within AIM.

18. Receipt and Acceptance of Information Technology Assets

18.1. The Prompt Payment Act (PPA) of 21 May 1982 (Public Law 97- 177), amended on 17 October 1988 (Public Law 100-496), 31 U.S.C. §3900, requires Federal agencies to pay commercial vendor bills on time and pay interest when payments are late. Consequently, the Air Force is subject to interest penalties if the proper invoice and receiving reports for IT assets are not processed in a timely manner. To ensure prompt payment to vendors and prevent interest penalties, SAF/FMP mandates the use of Wide Area Workflow (WAWF) to electronically submit all receiving reports to the DFAS.

18.2. All personnel receiving or accepting IT assets on behalf of the Air Force, usually the ECO, will ensure receiving reports for IT assets are processed using WAWF.

18.2.1. Receiving reports will be processed through WAWF within 3 working days of receipt and acceptance.

18.2.2. In those instances where the ECO or the person who received the IT does not have visibility of the order in WAWF, contact the unit Resource Advisor to ensure payment through appropriate channels.

18.3. If your organization cannot use WAWF, manually complete the receiving report by filling in the appropriate blocks of the DD Form 250, *Material Inspection and Receiving Report*, and forward a copy to your local FM Accounting Liaison Office (ALO) for processing to WAWF within 3 working days of IT asset receipt and acceptance.

18.4. Training on the use of WAWF is available using the Department of Defense Receipts & Acceptance online training system at <http://www.wawftraining.com> or you can contact your local or host Comptroller office to schedule additional WAWF training.

18.5. Recommend those submitting purchase requests ensure existence of a WAWF Business Partner Network (BPN) number at <http://www.bpn.gov/>. BPNs are the equivalent to DoDAACs and are the critical data link in identifying the responsible organization to accomplish a WAWF receiving report.

18.6. Following IT asset receipt and acceptance, accountability must be established for the IT asset. According to DoD Instruction (DoDI) 5000.64, *Accountability and Management of DoD Owned Equipment and Other Accountable Property*, dated 2 Nov 2006, accountability is established by formal receipt and acceptance in an accountable property system of record. For IT hardware assets, the Air Force's official accountable property system of record is the AFEMS-AIM module.

18.7. To ensure the ECO enters IT assets into the AFEMS-AIM system in a timely manner and establishes accountability in accordance with DoDI 5000.64, the following applies:

18.7.1. The ECO, or supporting personnel, will enter newly received IT assets into the AFEMS-AIM system within 10 working days of receipt and acceptance.

18.7.2. For equipment not immediately installed, the ECO will use the appropriate IT asset status code in accordance with AFI 33-112, Attachment 3 (i.e., Status Code 03 - Received on-site, but not installed.)

18.7.3. If the receiver/acceptor of the IT asset is not the ECO, 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.

19. Establishing Custodial Responsibility.

19.1. In order to effectively control Air Force IT assets, custodial responsibility must be established at all levels. Custodial responsibility is established when an individual takes physical custody of the property and signs a custody receipt document such as an AFEMS-AIM inventory list or a hand receipt. Digital signatures may be used in lieu of wet signatures.

19.2. 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.

19.3. There are two methods to establish custodial responsibility.

19.3.1. Establish an organizational IT asset equipment account in AFEMS-AIM.

19.3.1.1. The organizational commander or equivalent appoints an ITEC for the account according to paragraph 8.5 of this instruction.

19.3.1.2. The ITEC accepts custodial responsibility on behalf of the organization by signing an AFEMS-AIM inventory list provided by the ECO. Digital signatures may be used in lieu of wet signatures.

19.3.1.3. The ITEC conducts the annual physical inventory according to this AFI.

19.3.1.4. It is highly recommended that ITECs have end users sign a hand receipt for the IT in the user's possession or IT they use on a regular basis. At a minimum, hand receipts must be accomplished for easily transported devices such as laptops and PDAs. Digital signatures may be used in lieu of wet signatures.

19.3.1.4.1. Hand receipts may be as simple as AF Form 1297, *Temporary Issue Receipt*, or as elaborate as a digitally signed electronic hand receipt. The hand receipt must state, "I acknowledge receipt of and responsibility IAW AFI 23-111 for the items listed herein."

19.3.2. Upon MAJCOM A6 approval, CSOs may allow 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 traditional ITECs. Use of hand receipts for this method is mandatory.

19.3.2.1. The user will sign the hand receipt acknowledging custodial responsibility and will in effect become the equipment custodian for the property listed on the hand receipt. Digital signatures may be used in lieu of wet signatures.

19.3.2.2. The Commander of the organization will certify the annual inventory. This date will be used as the official inventory date in AFEMS-AIM.

20. Physical Inventory of IT Hardware Assets.

20.1. A physical inventory is a process in which the actual existence, location, and quantity of IT assets are validated against the inventory records in AFEMS-AIM.

20.2. During the inventory, record deficiencies, such as incorrect locations or unrecorded property items are identified and these records are corrected as part of the process. Finally, physical inventory serves as a deterrent to loss, theft, damage, and misuse.

20.3. Official Air Force validation techniques include: hands-on verification, barcode scanning, radio frequency identification (RFID), and network log-on or use records using network auto-discovery tools.

20.4. 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.

21. Transferring Non-excess Information Technology (IT) 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. BRAC), and the IT assets acquired to support that function, is transferred to another DoD component or Federal agency.

21.1. The losing ITEC provides the losing ECO with a letter of transfer, signed by the losing commander documenting the transfer of the function and equipment.

21.2. 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 ITEC. For local transfers where no shipping activity is involved, the gaining and losing ITEC signs the DD Form 1149.

21.3. The ECO for the losing activity should account for the transferred IT. The ECO should also identify excess IT created as a result of the transfer of a function.

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

21.3.1.1. Review contracts to terminate maintenance for excess equipment.

21.3.1.2. Assist contracting officials in the transfer of responsibilities to the gaining activity.

21.4. The losing ECO will:

21.4.1. Update the asset status field in AFEMS-AIM using the codes in Attachment 3.

21.4.2. Provide information for accountable records to the gaining activity if the gaining activity is not using the same database as the losing activity.

21.4.3. Review all contract obligations with the gaining and losing activity. 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.

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

21.4.5. Coordinate IT assets release dates with other base functions, if necessary.

21.4.6. Coordinate with ISSO for hard drive sanitization according to the procedures outlined in AFSSI 8580.

21.4.7. Provide the IT system database records or custodian report for the ITEC to attach to the equipment being transferred as appropriate.

21.4.7.1. The ITEC will place all applicable hard copy records regarding the transfer in their applicable ITEC folder.

21.4.8. Properly inventory, package, warehouse, and secure equipment when storing IT assets before transfer.

21.4.9. Ensure the IT system database inventory records reflect this transfer of equipment accountability to the receiving organization.

21.4.10. Ensure the AFEMS Help Desk is notified to delete or archive the IT records of the equipment being transferred to a Department of Defense Component, Federal Agency, State, or Local Government.

22. Managing Capital Assets

22.1. The Chief Financial Officer (CFO) Act of 1990, 31 U.S.C. §§901-903, specifies capitalization and depreciation of equipment with an acquisition/leased cost equal to or greater than \$100K. 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 Air Force Financial statement that is submitted to Congress.

22.1.1. Acquisition cost, which is what depreciation is based on, includes all costs incurred to bring the asset to a form and location suitable for its intended use (e.g.,

amounts paid to vendors, transportation to point of initial use, handling and storage costs, interest costs paid, and direct and indirect production costs). The acquisition cost is typically found on an accompanying invoice.

Section D—Information Technology (IT) Systems Maintenance (Not Applicable to Non-Air Force Managed Joint Service Systems)

23. Support Plans. The CSO develops a Life Cycle Management Plan for IT assets according to AFI 63-101, *Acquisition and Sustainment Life Cycle Management* to ensure logistics support throughout the expected lifecycle. 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.

23.1. Although there is no one size fits all 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/commercial off-the-shelf systems that determine the number of on-hand spares necessary to ensure mission accomplishment.

23.1.1. 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 Life Cycle Management Plan.

Note: Consult AFI 33-115, Volume 1, for additional guidance in determining types and quantities of equipment needed.

23.2. 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 requirements (Refer to AFI 63-101, AFI 33-115, Volume 1, and AFI 33-series guidance).

23.3. Personnel performing maintenance tasks on IT hardware follow the maintenance management requirements for mission critical and non-mission critical items according to TO 00-33A-1001, *General Communications Activities Management Procedures and Practice Requirements*.

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

23.5. Cannibalization may be used to satisfy an existing requirement or to meet priority mission requirements. Technical Order 00-20-3, *Maintenance Processing of Repairable Property and Repair Cycle Asset Control System*, outlines the cannibalization process and documentation requirements.

23.6. When cannibalization is the only option available, identify the end item to be cannibalized, and request approval from the chief of maintenance/chief of mission systems flight, CSO, or designated representative according to TO 00-20-2, *Maintenance Data Documentation*.

23.7. The CSO or designated representative can approve cannibalization of non-mission critical IT equipment; however, the CSO ensures procedures are developed to ensure non-mission critical cannibalized IT assets are restored to full operational capability if economically feasible.

23.8. Maintenance actions to obtain assemblies, sub-assemblies, or parts are considered transfers and are not treated as cannibalization actions. The CSO 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.

23.9. The CSO 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.

23.10. 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 3.

24. Information Technology (IT) Systems Maintenance Reporting. Users with maintenance contracts document all IT asset maintenance on AF Form 597, or vendor maintenance forms as specified in the appropriate contract. If AF Form 597 is used, provide a copy to the vendor. Each MAJCOM CIO/A6 will specify procedures for logging, documenting, collecting, processing, and filing copies of maintenance records in accordance with AFI 33-300 series publications.

25. Computation of Payments. Contracts applying to managed IT assets.

25.1. 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.

25.2. Computing Charges. ECOs compute charges for rented/leased IT assets, using the reverse side of AF Form 597 or locally produced vendor form.

25.3. Validating Services. For Air Force-managed systems, the verifying activity refers to the equipment utilization reports and the input to the reports (IT assets/equipment orders, AF Form 597, 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-Air Force managed systems (e.g., joint service systems).

Section E—Disposition of Excess Information Technology (IT) Resources

26. Excess. 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 Life Cycle Management Plan. According to AFI 23-111, accountable individuals are responsible for

properly identifying, reporting, and determining correct disposition of unserviceable, repairable, or excess property.

26.1. Base or MAJCOM CSOs may develop their own policies for the retention of excess IT assets, to include potential reutilization (see AFSSI 8580). However, the rationale for the retention policy must be documented; preferably in the Life Cycle Management Plan.

26.2. The ITEC notifies the ECO when IT assets become excess. If possible, ITECs should provide notification 30 calendar days before the equipment goes off line to allow completion of the screening cycle while the equipment is still in use, eliminating the need to store excess assets. Until receipt of final disposition instructions, the ITEC stores the equipment to prevent damage, deterioration, or unauthorized cannibalization.

26.3. Excess Air Force assets can be located using DLA Disposition Services (formerly DRMO) at <http://www.drms.dla.mil/>.

26.4. Disposition of excess classified media. The ISSO or designated representative signs and affixes the appropriate disposition certification label and marks classified media as required according to the guidance in AFI 31-401, *Information Security Program Management*. Also, all personnel handling classified materials bear a responsibility to ensure their media is appropriately marked. **Note:** For your use, DLA has developed a label, based on the information required in Assistant Secretary of Defense (ASD) Memorandum, *Disposition of Unclassified DoD Computer Hard Drives*, June 4, 2001. This is an optional form. Please note that it also contains a block to check if you are turning in housings where the hard drive has been removed. This form can be printed on adhesive labels, i.e., Avery 5164 or Pres-a-ply 30604 (reference AFSSI 8580 and AFI 31-401).

27. Obtaining Excess Resources. If the parent MAJCOM allows the use of excess IT to satisfy new requirements, the ECOs review excess redistribution programs and reports to determine if suitable excess resources are available.

27.1. The ECO may direct reutilization of IT assets to replace equipment that does not meet minimum standards when allowed by the parent MAJCOM.

27.2. To acquire equipment from DLA Disposition Services (formerly DRMO), the ITEC submits documentation (DD Form 1348A-1, *Issue Release/Receipt Document*) for coordination to the ECO. Assets can either be viewed at the DLA Disposition Services (formerly DRMO) location or researched at <http://www.drms.dla.mil/>.

27.3. ECOs establish accountability in the AFEMS-AIM for IT hardware equipment acquired through any source that meets the criteria for accountability in paragraph 17.

28. Transferring Excess Information Technology (IT) Systems Assets to the DLA Disposition Services (formerly DRMO).

28.1. DLA Disposition Services (formerly DRMO) is the primary source for disposal of all military property and equipment. All Air Force IT will be disposed of through the DLA Disposition Services (formerly DRMO).

28.2. DLA Disposition Services (formerly DRMO) guidelines for excess and the disposal of IT assets can be found at <http://www.drms.dla.mil/>

28.3. All media being disposed of or transferred to DLA Disposition Services (formerly DRMO) or another entity outside of the DoD will be sanitized and/or destroyed as applicable according to AFSSI 8580.

28.4. ECOs must establish an MOA with their servicing DLA Disposition Services (formerly DRMO) 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 DLA Disposition Services (formerly DRMO).

28.4.1. The Air Force cannot donate IT assets directly to a school or other government entity without the approval of the DLA Disposition Services (formerly DRMO).

29. Exchange or Sale of Government Automated Resources.

29.1. Contract partners have programs designed to recover (give credit for equipment that still has market value) and recycle (dispose of IT assets in an environmentally safe manner and replace due to obsolescence or un-serviceability) IT 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, May 23, 2003; and Defense Federal Acquisition Regulation (DFAR) Supplement, Part 217.70, Exchange of Personal Property, for more specific guidance. Adherence to remanence security requirements is vital to all transactions relating to excess IT including warranty exchanges.

30. Information Collections, Records, and Forms.

30.1. Information Collections. No information collections are created by this publication.

30.2. Records. The program records created as a result of the processes prescribed in this publication are maintained in accordance with AFMAN 33-363 and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at <https://www.my.af.mil/afrims/afrims/afrims/rims.cfm>.

30.2.1. IT Asset Management documents: use Table 33-7, Rule 7 is delete when no longer needed. Recommend keeping inventories and supporting documentation for two years, when possible.

30.3. Forms (Adopted and Prescribed):

30.3.1. Adopted Forms: DD Form 200, *Financial Liability Investigation of Property Loss*; DD Form 1149, *Requisition and Invoice/Shipping Document*; DD Form 1348A-1, *Issue Release/Receipt Document*; AF Form 847, *Recommendation for Change of Publications*; AF IMT 2519, *All Purpose Checklist*.

30.3.2. Prescribed Forms: AF IMT 597, *ADPE Maintenance Record*; AF Form 1297, *Temporary Issue Receipt*.

Chief of Warfighting Integration and Chief
Information Officer

PAUL A. WELCH, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

- (Added-688IOW) DoD Regulation 5200.40, *DoD Information Technology Security Certifications and Accreditation Process*, 30 December 1997
- (Added-688IOW) Joint Department of Defense Intelligence Information System\Cryptologic SCI Information Systems Security Standards, 31 March 2001
- PL 104-52, *Telephone Installation and Charges*, STAT 468, Section 620 [31 U.S.C. 1348]
- ASD Memorandum, *Disposition of Unclassified DoD Computer Hard Drives*, June 4, 2001: [http:// www.drms.dla.mil/](http://www.drms.dla.mil/)
- DoDD 8000.1, *Management of DoD Information Enterprise*, February 10, 2009
- DoDI 5000.64, *Accountability and Management of DoD-owned Equipment and Other Accountable Property*, November 2, 2006
- DoDI 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003
- DoD 4140.1-R, *DoD Supply Chain Materiel Management Regulation*, May 23, 2003
- DoD 7000.14-R, Volume 12, *Special Accounts, Funds and Programs*, June 2009
- (Added-688IOW) AFMAN 33-363, *Management of Records*, 1 March 2008
- (Added-688IOW) AFI 33-101, *Communications and Information Management Guidance and Responsibilities*, 18 November 2008
- AFPD 10-6, *Capabilities Base Planning & Requirements Development*, May 31, 2006
- AFPD 20-1, *Acquisition and Sustainment Life Cycle Management*, April 3, 2009
- AFPD 33-1, *Information Resource Management*, June 27, 2006
- AFPD 33-2, *Information Assurance (IA) Program*, April 19, 2007
- AFPD 65-2, *Managers' Internal Control Program*, April 28, 2006
- AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program*, December 1, 2004
- AFI 23-111, *Management of Government Property in Possession of the Air Force*, July 25, 2005
- AFI 31-401, *Information Security Program Management*, November 11, 2005
- AFI 31-501, *Personnel Security Program Management*, January 27, 2005
- AFI 33-103, *Requirements Development and Processing*, March 18, 1999
- AFI 33-114, *Software Management*, May 13, 2004
- AFI 33-115, Volume 1, *Network Operations (NETOPS)*, May 24, 2006
- AFI 33-200, *Information Assurance (IA) Management*, December 23, 2008
- AFI 63-101, *Acquisition and Sustainment Life Cycle Management*, April 17, 2009

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

AFSSI 8580, *Remanence Security*, November 17, 2008

AFWay Users Guide, May 2007

FAR 7.5, *Inherently Governmental Functions*, June 15, 2009

FAR 45.505, *Records and Reports of Government Property*, June 15, 2009

FPM Letter 368-1, 26 March 1991, *Federal Flexible Workplace Project*, March 26, 1991

Technical Order 00-20-2, *Maintenance Data Documentation*, June 15, 2003

Technical Order 00-20-3, *Maintenance Processing of Reparable Property and Repair Cycle Asset Control System*, January 1, 2009

Technical Order 00-33A-1001, *General Communications Activities Management Procedures and Practice Requirements*, July 17, 2009

(Added-688IOW) AF Form 847, *Recommendation for Change of Publication*, 22 September 2009

Abbreviations and Acronyms

AF—Air Force (used on forms only)

AFEMS—Air Force Equipment Management System

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFNIC—Air Force Network Integration Center

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

AFSSI—Air Force Systems Security Instruction

AFWay—Air Force Way

AIM—Asset Inventory Management

(688IOW) AIM—Asset Inventory Management

AIS—Automated Information System

ANG—Air National Guard

ASD—Assistant Secretary of Defense

BRAC—Base Realignment and Closure

CAGE—Commercial and Government Entity code

CPU—Central Processing Unit

CSM—Computer Systems Management

CSMWG—Computer Systems Management Working Group

CSO—Communications and Information Systems Officer
(Added-688IOW) **CST**—Client Systems Technicians
DD—Department of Defense (used on forms only)
DFAR—Defense Federal Acquisition Regulation
DFAS—Defense Finance and Accounting Service
DLA—Defense Logistics Agency
DoD—Department of Defense
DoDAAC—DoD Activity Addressing Codes
(Added-688IOW) **DODIIS**—Department of Defense Intelligence Information System
DRA—Defense Reporting Activity
DRMO—Defense Reutilization and Marketing Office
DRU—Direct Reporting Unit
ECSS—Expeditionary Combat Support System
e-mail—Electronic Mail
EA—Economic Analysis
ECO—Equipment Control Officer
FAR—Federal Acquisition Regulation
FOA—Field Operating Agency
FOB—Found-On-Base
GO—General Officer
(Added-688IOW) **GSU**—Geographically Separated Unit
HTSA—Host Tenant Support Agreement
HQ AETC—Headquarters Air Education and Training Command
HQ OSSG—Headquarters Operations and Sustainment Systems Group
HQ SSG—Headquarters Standard Systems Group
IA—Information Assurance
ISSO—Information Systems Security Officer
IT—Information Technology
(Added-688IOW) **ITE**—Information Technology Equipment
ITEC—Information Technology Equipment Custodian
(Added-688IOW) **JDCSISSS**—Joint Department of Defense Intelligence Information System Cryptologic Sensitive Compartmented Information Systems Security Standards
LCMP—Life Cycle Management Plan

MAJCOM—Major Command

MECO—Major Command Equipment Control Officer

MOA—Memorandum of Agreement

OPR—Office of Primary Responsibility

PA—Program Agreement

PDA—Personal Digital Assistant

PL—Public Law

PMO—Program Management Office

RDS—Records Disposition Schedule

ROS—Report of Survey

SAF—Secretary of the Air Force

SAP/SAR—Special Access Program/Special Access Required

(Added-688IOW) SAV—Staff Assistance Visit

SES—Senior Executive Service

USAF—United States Air Force

WAWF— Wide Area Workflow

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.

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.

Central Processing Unit (CPU)—The portion of a computer that executes programmed instructions, performs arithmetic and logic functions, and controls input and output functions. One CPU may have more than one processor housed in the unit.

Client Support Administrator (CSA)—The primary point of contact for computer related problems. The person appointed and certified under AFI 33-115, Volume 1 to support information systems/technology related tasks. Formerly Workgroup Manager (WM).

Command, Control, Communications, and Computer (C4) System—An integrated system of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control through all phases of the operational continuum. This system includes visual information support systems. Within the Air Force referred to as communications and information systems.

Communications and Information Systems Officer (CSO)—The term CSO identifies the supporting systems officer at all levels. At base-level, this is the commander of the communications unit responsible for carrying out base communications and information systems responsibilities. At MAJCOM and other activities responsible for large quantities of communications and information systems, it is the person designated by the commander as responsible for overall management of systems budgeted and funded by the MAJCOM or activity. The CSO function uses the office symbol SC that is expanded to three and four digits to identify specific functional areas. CSOs are accountable officers for all automated data processing equipment in their inventory.

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.

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)—Official with the authority to formally assume responsibility for operating an information system or network within a specified environment. (AFI 33-200).

Documentation—The formal standardized recording of detailed objectives, policies, and procedures governing conception, authorization, design, testing, implementation, operation, maintenance, modification, and disposition of data administration techniques and applications.

Economic Analysis (EA)—An EA helps us make rational choices among competing alternatives. A good EA systematically examines and tells us about costs, benefits, and risks of various alternatives.

Equipment Control Officer (ECO)—An individual appointed by the applicable CSO 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.)

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 Systems Security Officer (ISSO)—Official who manages the computer security program for an information system assigned to him or her by the Information Systems Security Manager; including monitoring information system activities, and ensuring that the information system is operated, maintained, and disposed of according to security policies and practices. (NOTE: See DODI 8500.2, Information Assurance (IA) Implementation, February 6, 2003.) An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DoD information system or organization. While the term IAO is favored within the DoD, it may be used interchangeably with other IA titles (e.g., Information Systems Security Officer, Information Systems Security Custodian, Network Security Officer, or Terminal Area Security Officer). (AFI33-200).

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. (See DoD Directive 8000.1, Management of DoD Information Resources and Information Technology, February 27, 2002, with Change 1, March 20, 2002.) NOTE: The focus of this instruction is IT hardware management. AFI 33-114 is the governing Air Force instruction for software.

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.

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.

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 AIS that bases all programmatic decisions on the anticipated mission-related and economic benefits derived over the life of the AIS.

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

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.

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

Shareware—Privately or commercially developed software that is normally distributed free of charge but a fee is generally expected 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.

Attachment 2

INFORMATION TECHNOLOGY (IT) SYSTEMS CHECKLIST

A2.1. Information Technology (IT) Systems Checklist.

Table A2.1. Information Technology (IT) Systems Checklist.

#	ITEM	REFERENCE	Y	N	NA
	MAJCOM Equipment Control Officer (MECO)				
1	Has the MECO been appointed in writing? Has the letter been forwarded to the proper authority?	AFI 33-112, paragraph 9.1.			
2	Does the MECO provide policy and procedural guidance to ECOs and disseminate higher level guidance to the field?	AFI 33-112, paragraph 9.1.1 and 9.1.9.			
3	Does the MECO approve or disapprove transfers of IT assets between commands?	AFI 33-112, paragraph 9.1.3.			
4	Does the MECO review finalized excess reports to ensure appropriate actions are accomplished?	AFI 33-112, paragraph 9.1.5.			
5	Does the MECO maintain ECO appointment letters for each DRA under their command?	AFI 33-112, paragraph 9.1.7.1.			
6	Does the MECO approve system access requests for assigned ECOs?	AFI 33-112, paragraph 9.1.7.1.			
7	Does the MECO assist in the creation of new DRAs in their commands?	AFI 33-112, paragraph 9.1.7.			
	Equipment Control Officer (ECO)				
8	Is a copy of AFI 33-112 available?				
9	Has the CSO appointed a primary and alternate ECO in writing? Does the selected individual meet the criteria as noted in AFI 33-112?	AFI 33-112, paragraph 7.9.			
10	Does the ECO or ECO designated receiving official receive all AFEMS-AIM accountable IT equipment, ensuring accountability and completion of all necessary	AFI 33-112, paragraphs 10.2 and 18.2.			

	documentation?				
11	Does the ECO use AFEMS-AIM for accountable IT, according to AFI 33-112?	AFI 33-112, paragraph 10.2.1.			
12	Is the ECO responsible for equipment listed in their assigned DRA?	AFI 33-112, paragraph 10.2.2.			
13	Does the ECO assist the ITEC in determining ownership of all FOB IT assets and takes appropriate action to ensure accountability?	AFI 33-112, paragraph 10.2.3.			
14	Does the ECO direct all ITECs to conduct an annual physical inventory of assigned computer systems?	AFI 33-112, paragraph 10.2.4.			
15	Does the ECO ensure completion of the annual physical inventory and that ITEC appointment letters are reviewed annually?	AFI 33-112, paragraphs 10.2.4.			
16	Does the ECO prepare AFEMS-AIM generated or equivalent labels and provide them to the ITEC as needed?	AFI 33-112, paragraph 10.2.8.			
17	Does the ECO work with the ITEC to update the inventory as dictated by a ROS?	AFI 33-112, paragraph 10.2.9.			
18	Does the ECO complete out-processing for departing ITECs upon transfer of account and receipt of new appointment letters?	AFI 33-112, paragraph 10.2.10.			
19	Does the ECO provide guidance as well as initial and annual refresher training for the ITECs?	AFI 33-112, paragraph 10.2.11.			
20	Does the ECO receive guidance and direction from the MECO and CSO?	AFI 33-112, paragraph 10.2.12.			
21	Does the ECO correctly code deployed computer systems in AFEMS-AIM as directed by HQ USAF or MAJCOM and authorized by the applicable CSO?	AFI 33-112, paragraph 10.2.13.			
22	Does the ECO attempt to reutilize excess organizational IT assets that meet minimum architecture standards before offering	AFI 33-112, paragraph 10.2.15.			

	equipment to organizations outside the DRA, when allowed by the parent MAJCOM?			
23	Does the ECO work with tenant ECOs to establish a host tenant agreement identifying any assistance required, such as AFEMS-AIM connectivity?	AFI 33-112, paragraph 10.2.17.		
24	Does the ECO coordinate on all host tenant agreements?	AFI 33-112, paragraph 10.2.18.		
	IT Equipment Custodian (ITEC)			
25	Are ITECs and alternates appointed in writing by the organizational commander with signatures of appointees on letter?	AFI 33-112, paragraphs 8.5. and 8.5.1.1		
26	Are ITECs responsible for all assigned IT hardware assets?	AFI 33-112, paragraph 11.1.		
27	Do the ITECs perform an annual inventory of all items in the account not to exceed 365 calendar days? Upon completion, does the ITEC and the organizational commander or equivalent sign the inventory with the original copy retained by the ITEC and a copy for the ECO file?	AFI 33-112, paragraph 11.1.1.		
28	Does the ITEC ensure all AFEMS-AIM accountable IT hardware equipment has an AFEMS-AIM generated or equivalent label attached when practical?	AFI 33-112, paragraph 11.2.		
29	Does the ITEC obtain approval and coordinate all potential transfers of computer systems between accounts with the applicable ECO? Note: ITECs have no authority to transfer computer systems outside their account.	AFI 33-112, paragraph 11.3.		
30	Does the ITEC sign for new equipment received through the ECO?	AFI 33-112, paragraph 11.5.		
31	Does the ITEC provide appropriate documentation to the applicable ECO to clear the	AFI 33-112, paragraph 11.7.		

	account of equipment that was shipped to another base/location, transferred to another account, donated to a school, or turned-in to DLA Disposition Services (formerly DRMO)?			
32	Has a joint physical inventory been accomplished prior to equipment account transfer?	AFI 33-112, paragraph 11.10.		
33	Does the ITEC out-process through the applicable ECO?	AFI 33-112, paragraph 11.9.		
34	Does the ITEC initiate the ROS process according to AFMAN 23-220, concerning any lost, damaged, or destroyed IT assets?	AFI 33-112, paragraph 11.11.		
35	Does the ITEC provide the applicable ECO a serialized numbered list of UTC tasked assets that will deploy?	AFI 33-112, paragraph 11.13.		
36	Does the ITEC receive and secure all IT assets, if not received by the ECO, until proper accountability is established?	AFI 33-112, paragraph 11.14.		
37	Are easily transported devices (i.e. laptops, PDAs) signed out on hand receipts?	AFI 33-112, paragraph 19.3.1.4		

Attachment 3**EQUIPMENT STATUS REPORTING**

A3.1. The status codes in Table A3.1. describe the operational status of a component or DRA. Valid values are:

Table A3.1. 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.