# DCMA Manual 4401-17

# Information Technology Asset Lifecycle Management

==========

| | |
|---|---|
| **Office of Primary Responsibility** | **Organizational Infrastructure Capability Board** |
| **Effective:** | September 6, 2024 |
| **Releasability:** | Cleared for public release |
| **New Issuance** | |
| **Implements:** | The IT Asset Management scope of DCMA Instruction 4401, "Information Technology Management," January 20, 2020 |
| **Incorporates and Cancels:** | DCMA Instruction 803, "Workstation Peripherals & Consumable Supplies Below $500, August 11, 2011, as amended<br>DCMA Instruction 810, "DCMA-IT Acquisitions - Non-Programmed Acquisitions Valued at $3,000 or Below," November 22, 2011, as amended |
| **Internal Control Plan**: | Linked on the Resource Page for this Issuance |
| **Labor Codes:** | Located on the Resource Page |
| **Resource Page Link:** | https://dod365.sharepoint-mil.us/sites/DCMA-BCF-Information_Technology_Management/SitePages/4401-17r--Asset%20Lifecycle%20Management.aspx |
| **Approved by:** | G. L. Masiello, Lieutenant General, U.S. Marine Corps, Director |

**Purpose:** This issuance, per DoD Directive 5105.64, DoD Instruction 5000.64, and DoD Instruction 8440.01, implements policy, assigns responsibility, contains required amplification/detail, and/or relies upon other agency issuances to avoid gaps in meeting the entirety of these higher-level requirements, and provides clarity of and prescribes general principles and procedural direction associated with the visibility and tracking of accountable property and equipment through DCMA's Information Technology Asset Management framework. Implementation:

- Positions IT to better enable and enhance the virtual workspace of the future through Information Technology Asset Management accountability, best practices, and services
- Establishes Information Technology Asset Management activities and standards to manage risk, leverage opportunities, maximize benefits, drive performance, and form enduring strategies in support of strategic goals
- Provides for the responsible use, stewardship, management, security, and accountability of Information Technology property, including hardware, commercial software, DoD-owned internal use software, automated data processing equipment, and multi-functional devices
- Defines roles and responsibilities within DCMA Information Technology, property managers, program managers, and other officials
- Ensures sustainment of enterprise operations through accountability
- Assures compliance with" the FMR DoD 7000.14-R Volume 4, Chapter 6, and the Federal Accounting Standards Advisory Board's Statement of Federal Financial Accounting Standards Number 10
- Implements software financial reporting policy for DCMA per DoD Instruction 5000.76, Section 3.3 (4).

# TABLE OF CONTENTS

# SECTION 1: GENERAL ISSUANCE INFORMATION

## 1.1. APPLICABILITY.

This issuance applies to all DCMA activities unless higher-level regulations, policies, guidance, or agreements take precedence.

## 1.2. POLICY.

This Manual implements policy, assigns responsibility, and prescribes general principles of accountable property and available equipment. It provides guidance and direction for the operational management of information technology (IT) hardware and software. It is DCMA policy to execute this Manual in a safe, efficient, effective, and ethical manner within DCMA workplaces.

# SECTION 2: ROLES AND RESPONSIBILITIES

## 2.1. EXECUTIVE DIRECTOR AND CHIEF INFORMATION OFFICER (CIO).

The Executive Director and CIO of the DCMA Information Technology (DCMAIT) Directorate will:

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

b. Resolve management issues and policy disagreements between Centers, functional managers, and non-DCMA agencies for IT hardware and software assets.

c. Identify formal ITAM, hardware, and software management training requirements and provide them to the DoD CIO for incorporation into formal courses or virtual, professional continuing education learning curriculums.

d. Survey, consolidate, validate, and track DCMA requirements for potential DCMA enterprise software licenses for Commercial Off-The-Shelf (COTS) software.

e. Recommend software product candidates for potential DCMA-wide or DoD-wide licensing to the DCMA Capabilities Board. The DCMA Capabilities Board is responsible for securing approval and providing support, whether through Defense Information Technology Contract Organization (DITCO) or DCMA Contracts Directorate, for procuring enterprise licenses.

f. Serve as the DCMA Software License Manager to review and consolidate DCMA software license inventory (includes locally owned software and software yet to be transferred to an enterprise software license agreement).

g. Designate an IT Corporate Support Division as the Office of Primary Responsibility (OPR) for managing the DCMA Enterprise Software License Program (in coordination with the DoD CIO), and when designated, act as Executive Agent for establishing DoD-wide enterprise software license agreements.

h. Designate the Director, DCMAIT Corporate Support Division, as the centralized purchasing agent for software licenses to support consolidated and programmatic DCMA requirements.

i. Designate the Director, DCMAIT Corporate Support Division, to manage the commoditized purchase of DCMA infrastructure and platform service components. DCMAIT-Operations Division establishes DCMA enterprise commoditized purchasing and provisioning of infrastructure which ensures the management of IT assets within the infrastructure.

j. Serve as the Defense Accrediting Authority with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

k. Ensure that the DCMA Financial Business Systems Operations Branch appropriately manages the Defense Agencies Initiative (DAI) construction-in-progress (CIP) clearing process and reports capital software on DCMA financial statements quarterly. Once IT places an asset in service, Financial Business Systems Operations Branch will move CIP account recorded costs to the asset account.

**2.2. ITAM LEAD.**

The ITAM Lead will:

a. Conduct the daily operations of DCMA ITAM.

b. Serve as the DCMA ITAM Governance Board Chair.

c. Schedule Product and Service owner presentations to the DCMA ITAM Governance Board.

d. Serve as lead for implementation of ITAM and software management policies.

e. Develop and implement the DCMA-wide IT hardware and software management system providing a DCMA Configuration Management Database (CMDB). The CMDB:

(1) Enables DCMA implementation of the Information Technology Infrastructure Library practices for Software Asset Management (SAM) per International Standardization Organization/International Electrotechnical Commission (ISO/IEC) 20000-1, Information Technology – Service Management.

(2) Supports DCMA Configuration Management in accordance with (IAW) ISO/IEC 19770, SAM.

(3) Contains all DCMA hardware inventory, infrastructure configuration information, COTS entitlements, and software implementation metrics.

f. Assure IT asset inventory information is associated and/or synchronized to provide the complete picture of the IT asset lifecycle between the CMDB, Managerial System/Accountable Property System of Record (APSR), acquisition purchasing databases, financial databases, and any other systems requiring an authoritative data source for IT capital asset information.

g. Coordinate with the DCMAIT Field Services Center Director to establish and provide proper training, to include a learning map of the CMDB database, and fulfill ITAM oversight responsibilities.

h. Publish DoD ITAM and software metrics for IT hardware and software entitlements and implementation.

i. Manage DCMA Approved Software and Hardware Lists and make them available through the DCMA homepage or Service Center so users understand what certified COTS software products DCMA allows on DCMA assets.

j. Consolidate non-enterprise software inventories.

k. Ensure all software license requirements are purchased using approved DoD/DCMA Enterprise License Agreements (ELAs) through the DoD Enterprise Software Initiative (ESI), National Aeronautics Space Administration (NASA) Solutions for Enterprise-Wide Procurement (SEWP), or similar DoD-wide or Government-wide Acquisition Contracts.

l. Coordinate new license agreements/requirements with the governing Capabilities Board, Change Control Board, and IT Asset Manager (IT-AM).

m. Serve as responsible agent for the overall management of the DCMAIT hardware asset management program.

n. Provide guidance and procedures to the Directorate Accountable Property Control Officers (DAPOs) on the management of IT hardware assets.

o. Assist IT Divisions to ensure all hardware and software are purchased according to Paragraph 3.2. for hardware and Paragraph 4.2. for software.

p. Assist supporting Procurement Contracting Officers or their designees in determining requirements and developing an acquisition strategy for maintenance contracts, as required.

q. Provide technical/functional expertise, advice, and support to contracting officers for preparing requests for quotation, request or quotation response review, solicitation, and source selection actions.

r. Adhere to budgeting agreements and arrangements established in fiscal budgets.

s. Develop and maintain the ITAM Governance Board resources (process, internal controls, etc.) on this policy's resource page.

## 2.3. ORGANIZATIONAL ACCOUNTABLE PROPERTY OFFICER (APO).

The APO will:

a. Provide overall accountability and reporting of all DCMA Internal Use Software (IUS), mission software, test software, and IT hardware, regardless of category or location.

b. Ensure that the recorded cost of an asset in the Defense Property Accountability System (DPAS) includes all amounts captured on the receipt and acceptance documentation.

c. Assist the Finance and Accounting Officer (FAO) in establishing, reconciling, and maintaining financial records of all IUS, mission software, test software, and hardware as required by regulation or law.

d. Ensure Organizational APOs create DPAS due-ins and manage lifecycle transactions of IUS, mission software, test software, and hardware in their assigned accountable area or under their administrative control.

e. Process all forms received from the Property Administrator (PA) in DPAS.

**2.4. PA.**

The PA will:

a. Ensure that the System Authorization Access Request (DD Form 2875), User Agreement Form, Role(s) Request Form, and Computer Security/Information Assurance (IA) Awareness Training certificates are complete and accurate.

b. Send all forms to the APO for processing and to DPAS for access and training.

**2.5. ACCOUNTING SPECIALIST**

The Accounting Specialist will:

a. Create capital project subtasks in DAI for IUS, mission software, test software, and hardware that meet the capitalization criteria to establish the financial structure.

b. Establish separate requisition line items in DAI for IUS, mission, test software, and hardware.

c. Provide a copy to the APO on the obligation of funding in DAI to create DPAS due-ins. Proper receiving and identification of property require a DPAS local due-in.

**2.6. NON-TACTICAL VEHICLE (NTV) FLEET MANAGER.**

The NTV Fleet manager will:

a. Institute a management program for Enterprise NTVs that maximizes utilization and improves efficiency of NTVs throughout CMOs within CONUS and OCONUS, (refer to the DCMA Manual (DCMA-MAN) 4101-05, “Enterprise Non-Tactical Vehicles,” for additional preparation actions).

b. Report all accidents that result in a financial loss to the Government.

c. Report gains and losses of NTV’s to the APO.

d. Maintain the Maintenance and Utilization reports in an APSR.

e. Ensure fleet managers are hand-receipting vehicles on a DD Form 1150, "Temporary Issue Receipt." The Government Services Administration (GSA) Form is approved to hand receipt vehicles issued out for less than 72 hours.

## 2.7. FACILITIES PROPERTY MANAGER.

The facilities property manager will notify the APO in writing when fixed assets, including leasehold improvements, are projected to become DCMA property, as outlined in DCMA-MAN 4101-04, "Accountable Property & General Equipment."

## 2.8. CHIEF, IT ASSET MANAGEMENT.

The Chief, IT Asset Management will, as outlined in DCMA-MAN 4101-04**:**

a. Provide guidance and clarification regarding Federal and DoD policies associated with information management and IT investment policies and processes.

b. Manage DCMA general service systems, including IUS.

c. Provide transfer, disposal, or cancellation documentation of IUS to the FAO and APO.

d. Serve as the primary process owner for IT equipment and oversee development, implementation, administration, and management of the workstation peripherals and IT equipment.

## 2.9. CONTRACTING OFFICER'S REPRESENTATIVE (COR).

The CORs will:

a. Execute and manage the software acquisition activities throughout the entire lifecycle IAW the approved Program Software Acquisition Process Plan.

b. Identify how software builds (delivery of qualified software) will be grouped according to the software lifecycle, assign a useful life, and provide the beginning and end date for each software delivery. Amortization of a software project begins when a build has been tested (successfully) and formally qualified in the software test report.

c. Ensure the statement of work (SOW) or performance work statement (PWS) clearly identifies IUS, mission software, test software, and hardware that meet the capitalization criteria.

d. Notify the contracting officer of IUS, mission software, test software, and hardware that meet the capitalization criteria.

e. Assist the acquisition team lead and contracting officer in completing all documentation, including the software and hardware technical item description, estimated useful life, and estimated delivery date.

**2.10. IT FIELD SERVICES TEAM CHIEF**.

The IT Field Services Team Chief will:

a. Have the authority to submit documentation to the IT Accountability Property Officer (IT-APO) for deletion of Unit Identification Codes (UICs) and equipment from DPAS.

b. Submit DCMA Base Lateral Transfer Memos to transfer all UIC and equipment to the IT-APO for approval.

c. Ensure all UICs for deletion do not have property associated with them. Transfer the property or have an approval letter from Facilities for deletion. Facilities will provide APO with an approval letter to remove the UICs or equipment from DPAS. Upon receipt of a Facilities approval letter, the IT-APO will delete UICs and equipment.

d. Provide guidance and clarification regarding Federal and DoD policies associated with information management and IT investment policies and processes.

e. Manage DCMA general service systems, including Automated Data Processing (ADP) Equipment.

f. Provide transfer, disposal, or cancellation documentation of ADP equipment to the APO and FAO.

g. Serve as the primary process owner for all IT equipment and oversee development, implementation, administration, and management of workstation peripherals and IT equipment.

**2.11. IT-APO.**

The IT-APO will:

a. Serve as the primary IT-APO and alternate CPL for all IT hardware assets within DCMA.

b. Provide guidance and support to DCMA ITAM in managing IT hardware assets.

c. Review, evaluate, and interpret issues and problems as the IT-APO subject matter expert and make recommendations on IT-APO policy changes to the ITAM.

d. Act as IT-APO functional manager for the Managerial System/APSR for all proposed upgrades and/or modifications to the Managerial System/APSR.

(1) Maintain the list of designated IT/DAPOs.

(2) Manage the Managerial System/APSR accounts for DAPOs, including approving new account requests and freezing non-compliant accounts.

e. Approve asset transfers between Centers.

f. Manage the implementation of DoD and DCMA policy on Serialized Item Management and Item Unique Identification (IUID) for all IT hardware assets managed in the Managerial System/APSR.

g. Assist DAPOs in establishing or retiring new IUIDs (e.g., establishing or closing out an office or IT data system connectivity requests).

h. Freeze inventories for failure to comply with directions or procedures. Only resort to this option after providing the DAPO an opportunity to correct any deficiencies promptly due to the potential for a profound impact on an organization's mission.

i. Dispose of excess equipment IAW DoD Redistribution Program.

j. Be established as the Information Technology Information Owner IO responsibilities include:

(1) Work with component APO and verify all information contained in the APSR access request forms.

(2) Process forms and load them on the APSR File Upload site.

(3) Assist the Agency Primary CPL in completing DD Form 3042 and a bi-annual user audit inquiry.

## 2.12. IT DIVISON DIRECTORS.

IT Division Directors will:

a. Appoint at least one primary and alternate IT DAPO, document acknowledgment of duties with handwritten or digital signatures, and provide a copy to the IT-APO.

b. Notify IT-APO when the DAPO changes.

c. Manage assigned DAPOs.

d. Approve or reject transfer of IT hardware assets between Centers and coordinate with losing/gaining DAPO. The IT-APO will serve as a mediator when problems arise.

e. Approve or reject excess IT asset reports completed by DAPOs and ensure DAPOs complete appropriate actions.

f. Allow DAPOs to create and maintain holding accounts for known near-term requirements, as required.

g. Ensure the Managerial System/APSR inventory provides accountability of all IT hardware assets assigned to that UIC.

h. Assume accountability/responsibility for all DCMA enterprise assets on each UIC (e.g., gateway equipment, network infrastructure, defensive sensors, core service servers, laptops, printers, etc.). Each asset record should identify IT.

i. Annually conduct, certify, and document a hardware inventory IAW the provisions of this Manual. Provide a copy of the inventory to the IT-APO.

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

k. Serve as Appointing and Approving Official for Financial Liability Investigation of Property Loss (FLIPL).

**2.13. IT DAPO.**

The IT DAPO will:

a. Be appointed as primary or alternate by each IT Division Director (General Schedule - 15/Business Management and Technical Management Professional (NH) 4 equivalent). The DAPO cannot be the IT-APO or Personal Wireless Communications System (PWCS) Equipment Custodian for any DCMA account other than an account established for holding assets before distribution or disposal (i.e., holding, or excess accounts). (Ref. DoD FMR 7000.14-R, Volume 1, Chapter 4) All standard account management requirements apply (i.e., appointment letters, annual inventory, etc.) to these holding accounts.

b. Have the leadership skills and IT asset knowledge necessary to provide guidance and direction to the IT-APO.

c. Be a General Schedule-12 or higher for Primary DAPO. There is no grade requirement for an alternate DAPO.

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

e. Maintain currency in annual training.

(1) Document annual training and review currency in the Managerial System/APSR that should coincide with the annual inventory.

(2) At a minimum, training will include DAPO roles and responsibilities and any local policies for disposal, training, new item adds, etc.

f. Maintain a listing of DAPO appointments.

g. Manage all equipment listed in their assigned UIC.

h. Process the receipt and transfer of all IT assets and complete necessary documentation to establish custodial responsibility.

(1) Determine the ownership, reassignment, or disposition of all Found-on-Base IT assets.

(2) At a minimum, conduct a complete annual inventory of all IT hardware assets and/or PWCS assigned to the UIC.

(3) Provide IT-APO with Managerial System/APSR generated, IUID, or equivalent labels.

(4) Update inventories as required by FLIPL using the mandatory DD Form 200, "Financial Liability Investigation of Property Loss," to adjust accountable records.

(5) Deploy The Managerial System/APSR, Unit Task Code tasked IT assets at the request of the IT-APO or deployment authority.

(6) Use the Managerial System/APSR to accomplish the deployment.

(7) Monitor DCMA collaboration sites for additional guidance and support to ITAM. Access the link on the resource page.

(8) Perform periodic compliance visits to ensure effective accountability and asset management processes.

(9) Conduct a 100 percent joint inventory (can be a secondary DAPO or other designees with incoming primary DAPO) and reconcile any discrepancies and missing items via FLIPL or hand receipt no later than 30 days before a permanent change of station, permanent change of assignment, deployments (over 120 days), separation, or retirement. Upon discovery of lost, damaged, or destroyed assets:

(a) Notify the IT-APO and organization commander or equivalent.

(b) Report the loss of any IT hardware asset with persistent storage to the Information Systems Security Officer.

(c) Initiate the FLIPL process per DoD FMR Volume 12, Chapter 7.

(d) Provide the applicable IT-APO with a serialized numbered list of any Managerial System/APSR accountable assets considered for deployment.

(e) Ensure hard drives are sanitized based on the level of information contained within the media IAW DCMA-MAN 3301-08, "Information Security." For hard drives containing classified national security information, refer to DoDM 5200.01, Volume 3, and National Security Agency (NSA) / Central Security Service (CSS) Policy Manual 9-12, "Storage Device Sanitization and Destruction Manual utilizing the NSA Evaluated Products List (EPL). For hard drives containing Controlled Unclassified Information and Uncontrolled Unclassified Information, refer to DoD Instruction (DoDI) 5200.48, and National Institute of Standards and Technology (NIST) Special Publication 800-88 Rev. 1, "Guidelines for Media Sanitization. DCMA-MAN 3301-08, and National Institute of Standards and Technology (NIST) Special Publication 800-88 (as revised), "Guidelines for Media Sanitization", as applicable.

(f) Dispose of cellular devices used to process CUI or Unclassified Uncontrolled Information IAW DoDI 5200.48, and NIST Special Publication 800-88 (as revised), “Guidelines for Media Sanitization”.

(g) Turn-in excess cellular devices exposed to classified information to Defense Logistics Agency Disposition Services (DLADS) for destruction. Before sending cellular devices to DLADS for destruction, they must be wiped IAW DCMA-MAN 3301-08, DoDM 5200.01, Volume 3, “Protection of Classified Information”, and NSA/CSS Policy Manual 9-12, “Storage Device Sanitization and Destruction Manual utilizing approved products on the NSA EPL.

## 2.14. SOFTWARE LICENSE MANAGER/SOFTWARE ASSET MANAGER (SAM).

Each SAM will:

a. Ensure DCMA maintains a software inventory of all non-enterprise Government off-the-shelf software (GOTS)/COTS and associated licenses used by the organization IAW OMB 16-12, Category Management Policy: Improving the Acquisition and Management of Common Information Technology: Software Licensing, 2 June 2016, and other regulatory requirements.

b. Maintain a current list of all designated organization representatives.

c. Conduct annual inventories for all non-enterprise software licenses.

(1) Monitor the agency’s automated software inventories.

(2) Collect an annual baseline of an inventory for all non-enterprise software licenses certified by each Program Manager (PM)/Center Director.

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

d. Provide software license training for Service Center Customer Service Technicians (CSTs), IT Specialists, and other personnel managing software licenses.

e. Verify new acquisitions against the procedures in Section 4.

**2.15. CUSTOMER SERVICE TECHNICIAN/IT SPECIALIST.**

Each Customer Service Technician/IT Specialist will:

a. Refrain from obtaining or installing hardware or software without prior validation that DCMA approved the software or hardware for use and that a software license is available.

b. Ensure all networked computer systems comply (installed and managed by Group Policies) with the DCMA Standard Desktop Configuration.

c. Ensure limited user access/permissions on computer systems are imposed and maintained to enforce DCMA Standard Desktop Configuration integrity. Use an automated software tool to remove administrator rights as applicable.

**2.16. IT PM.**

The PM will:

a. Establish a central receiving and distribution point for accurate accountability throughout the lifecycle of IT software and hardware assets.

b. Execute and manage the software and hardware acquisition activities throughout the entire lifecycle IAW the approved Program Software Acquisition Process Plan.

c. Identify how software builds (i.e., delivery of qualified software) will be grouped according to the software lifecycle, assign a useful life, and provide the beginning and end date for each software delivery. Amortization of a software project begins when a build has been successfully tested and formally qualified in the software test report.

d. Ensure the SOW or PWS identifies IUS, mission software, test software, and hardware that meet the capitalization criteria.

e. Notify the contracting officer of IUS, mission software, test software, and hardware that meet the capitalization criteria. Assist the acquisition team lead and contracting officer in completing all documentation, including the software item description, estimated useful life, and estimated delivery date.

f. Provide all Hardware and Software contracts to IT-AM.

g. Validate with ITAM that Flexera correctly reflects all contract entitlements.

h. Direct the use of a hand-receipt, or automated process that meets the intent, as necessary for inventory control. Monitors will be considered accountable assets and tracked in The Managerial System/APSR.

## 2.17. PRIMARY STAKEHOLDER.

The Primary Stakeholder will:

a. Provide input to the ITAM Governance Board and work with Practice Leads, Functional Leads, Process Owners, and Service Owners to develop, implement, and improve IT services.

b. Serve as non-voting members of the ITAM Governance Board.

## 2.18. DCMA FINANCIAL AND BUSINESS OPERATIONS COMPTROLLER/CHIEF FINANCIAL OFFICER.

The DCMA Financial and Business Operations Comptroller/Chief Financial Officer assigned representative will:

a. Ensure appropriate integration of property management procedures with core financial systems and processes, particularly those for logistics and acquisition.

b. Ensure adequate internal controls over financial reporting and financial systems.

c. Periodically schedule internal reviews and audits for the Agency to assess property accountability management systems and inquiries involving property losses.

d. Ensure that all persons entrusted with government property are aware of the fiscal implications of improperly handling government furnished equipment. These responsibilities include proper care and stewardship of hardware and software and appropriate functional-level responsibility training.

e. Ensure that the Programming and Budget Office appropriately manages the DAI CIP clearing process and quarterly reports ADP Equipment on the DCMA financial statements. Once IT places an asset in service, the Programming and Budget Office will move the CIP account recorded costs to the asset account.

## 2.19. IT SPECIALIST/LOCAL IT SPECIALIST/CUSTODIAN.

The IT Specialist will**:**

a. Be responsible for the roles that fall under their location.

b. Submit a package for processing to the IT-APO that includes the DPAS Property Accountability Role Request, DD Form 2875, Cyber Awareness Certificate, and User Agreement forms.

c. Refrain from deleting equipment from DPAS asset receiving or transfers; these actions have no IT Specialist authority.

d. Sign DPAS custodian inventory report, verifying they have completed their location's total inventory.

e. Support the Financial Liability Officer during FLIPL.

**2.20. END USERS.**

End users will:

a. Maintain accountability and physically secure issued IT devices at all time IAW DCMA User Access Agreement and Rules of Behavior.

b. Acknowledge receipt of IT Government Furnished Equipment by signing DD Form 1150. By acknowledging this form, users agree to:

(1) Receive the item or items listed above on the date indicated.

(2) Accept personal responsibility for the property and surrender it upon demand, transfer, or separation from the Government.

(3) Understand that this property is for official use only and that I will comply with U.S. Government, DoD and DCMA rules, regulations and guidance concerning the appropriate use and safeguarding of U.S. Government property.

(4) Understand that failure on my part to exercise responsibility for the care and protection of the items listed above could result in pecuniary liability established IAW statute, regulation, and policy, to include Department of Defense Instruction 5000.64 and DoD 7000.14-R, Volume 12, Chapter 7.

c. Report Lost, Theft, Damaged, or Destroyed equipment. End users will immediately report lost, damaged, destroyed, or compromised IT equipment to:

(1) The DCMA Network Operations Center (NOC)

(2) The DCMA Service Center

(3) The IT Accountable Property Officer

(4) Supervisor

(5) A police report must be filed for stolen IT equipment. If not filed, end users will be held accountable for its replacement IAW DCMA-MAN 4101-04, "Accountable Property and General Equipment" and DoD 7000.14-R, Volume 12, Chapter 7."

# SECTION 3: HARDWARE ASSET MANAGEMENT

## 3.1. IT HARDWARE ASSETS AND INVENTORY MANAGEMENT.

### a. Accountability Determination.

Multiple and complex congressional, federal, DoD, and DCMA policies govern the accountability of hardware assets. Hardware assets may be hybrid devices with multiple uses, complicating the precise definition of a specific hardware type. An example of a hybrid device is a two-in-one personal computer with two distinct parts: a screen and a detachable keyboard. The screen can be used alone as a tablet, or together, they function as a laptop. Use the following to determine the accountability of IT assets based on acquisition cost thresholds and features of the hardware.

(1) Send concerns about including or excluding IT hardware assets in the Managerial System/APSR to the Asset Mailbox: dcma.gregg-adams.hq.list.dcma-it-asset-management-team@mail.mil.

(2) Access the email address on this manual's resource page.

### b. Sensitive IT Assets (Controlled Inventory Items).

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

(2) Sensitive IT assets must be accounted for in the Managerial System/APSR as commodity code "A" due to their capability to process and/or transmit personally identifiable information or other sensitive Agency information according to DoDI 5000.64. These items' physical accountability is required to support IT configuration management and IA requirements. Physical accountability endorses automating the association of IT assets with network configuration management items and enhancing overall situational awareness of physical assets for cybersecurity readiness.

(a) A FLIPL is required for the loss of any sensitive IT asset regardless of cost.

(b) Report the loss of any IT asset with persistent storage to the Information Systems Security officer within seven calendar days of the known loss. IAW local procedures, report lost/stolen devices to the Network Operations Team unless a DD Form 200 is on file.

**c. Non-Sensitive IT Assets.**

(1) Non-sensitive IT assets include peripherals and other IT hardware lacking both persistent storage and IP network capabilities (e.g., mouse, keyboard, monitor, non-network displays, non-network capable Keyboard Video Mouse switch, non-network capable fax machine, and non-network capable printer). Non-sensitive IT assets also include IT hardware providing Wireless Personal Area Network capabilities without IP network capabilities (e.g., wireless mouse and Bluetooth keyboard).

(2) Non-sensitive IT assets with a unit acquisition cost of $5,000 or more are accountable items and must be accounted for in the Managerial System/APSR.

(3) Non-sensitive IT assets with a unit acquisition cost of less than $5,000 may be tracked locally in the managerial system based on established Standard Operating Procedures (see DoDI 5000.64).

(4) If the Managerial System/APSR is used to track non-sensitive IT assets, a FLIPL is required to adjust those records in the Managerial System/APSR when a non-sensitive asset is lost, destroyed, or otherwise unaccountable.

**d. PWCS, including Commercial Mobile Devices (CMDs) and cellular phones.**

(1) Any PWCS hardware meeting the definition of sensitive IT assets (persistent storage or IP network capable) must be accounted for as sensitive IT assets (e.g., CMDs, mobile wireless devices, tablets) according to Paragraph 3.1.b.

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

(3) The Communications Security Responsible Officer will manage Type-1 CMDs and Secure Mobile Environment Portable Electronic Devices (PEDs).

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

## 3.2. HARDWARE ASSETS ORDERING AND PROCUREMENT GUIDANCE.

a. All IT hardware (including PWCS) will be procured using applicable DCMA Procurement Center or Defense Information Systems Agency (DISA) DITCO IT enterprise buying programs.

(1) All requests for hardware must comply with National Defense Authorization Act. A DoD unique identifying number must accompany the acquisition.

(2) DCMA may approve a Deep Packet Inspection waiver of the DCMA/DITCO process.

(3) Customers requiring equipment for Sensitive Compartmented Information Facilities (SCIFs) will order from the Evaluated/Approved Products Listing or other designated SCIF cognizant security authority representative before purchase.

(4) Defense Logistics Agency-Document Services is the preferred provider for printing services according to DoDI 5330.03.

(5) All hardware purchases will comply with Section 2222 of Title 10, United States Code (U.S.C.) and the most recent published Deputy Chief Management Office guidance for Defense Business Systems Funds Certification and Defense Business System Integrated Program/Budget Review.

b. Purchase request submitters will ensure a Wide Area Workflow (WAWF) Business Partner Network number is included (available under references on the resource page for this manual).

c. Ensure complete information is on shipping labels for ordered equipment. Obtain confirmation that procurement officials specify, as a contractual requirement, that "Ship To" and "Mark For" information is detailed on the shipping labels. This clarification will alleviate problems with receiving and accepting new hardware assets.

(1) "Mark For" information will identify the Contract Number, Purchase Order Number, Address, Phone Number, Email Address, Resource Manager Name, and IT-APO Name (when applicable).

(2) "Ship To" information will identify the complete delivery address. This includes the Equipment Control Officer's name, corresponding to the DoD Activity Address Code.

## 3.3. RECEIPT, ACCEPTANCE, AND MANAGING HARDWARE CAPITAL ASSETS.

a. IT asset accountability must be established by formal receipt and acceptance in an APSR according to DoDI 5000.64. DCMA's official APSR is DPAS as listed on the DD Form 3042 for hardware assets. IT asset accountability will be established on time by the following:

(1) IT Specialists will receive all assets centrally and report them to the DAPO. If any exception to this is required, receive and secure any assets not acquired by the IT Specialist until proper accountability is established. This practice will be the exception and not be the standard way of receiving property. Assets within SCIFs will follow the Intelligence Community Directive 503, Committee on National Security Systems Instruction 1253, or other policies issued by national intelligence community elements.

(2) The IT-APO, or designated alternate, will enter newly received IT assets into the Managerial System/APSR within ten working days of receipt and acceptance.

(3) IT-APO will enter the correct location code and ensure valid entry into the Managerial System/APSR for all assets in their UIC.

(4) For equipment not immediately installed, the IT-APO will use the appropriate IT asset status code (e.g., Status Code 03 - Received on-site but not installed).

(5) If the receiver/acceptor of the IT asset is not the DAPO, the receiver/acceptor will notify the DAPO upon receipt and acceptance of the IT asset so there is established accountability in the Managerial System/APSR system within ten working days of receipt and acceptance.

(6) IT-APO will establish unique asset identification (IUID) for each item according to Serialized Item Management and IUID guidance in DoDI 8320.03 and DoDI 8320.04.

(a) IUID/radio frequency identification (RFID labels will either be affixed to the asset by the manufacturer or applied by the IT Specialist.

(b) When the device is too small or the vendor does not ship with a label, user-generated labels that include the Commercial and Government Entity (CAGE) code, part number, and serial number will be used.

1. If the label placed by the manufacturer does not match the Managerial System/APSR data for the asset, then a label with the correct information matching the data in the Managerial System/APSR will be placed onto the item.

2. Equivalent labels will contain the asset's CAGE code, part number, and serial number.

(7) For holding accounts in the Managerial System/APSR, the DAPO login user record will not be used (this causes a system discrepancy when trying to make changes to the UIC). Establishing a central receiving and distribution point is mandatory for ensuring accurate accountability throughout the lifecycle of IT assets.

b. Federal agencies must pay commercial vendor bills on time and pay interest when payments are late IAW the DoD FMR 7000.14-R, Volume 10, Chapter 7, "Prompt Payment Act." Delayed and/or proper processing of IT asset invoices and receiving reports subjects DCMA to interest penalties. To ensure timely payment to vendors and avoid interest penalties, the use of WAWF is mandatory to electronically submit all receiving reports to the Defense Finance and Accounting Service (DFAS).

(1) All personnel receiving or accepting IT assets on behalf of the DAPO will ensure that receiving reports are processed using WAWF within three working days of receipt and acceptance.

(2) If the DAPO or the person who received the IT asset(s) needs visibility of the order in WAWF, they must contact the PM for the asset to ensure payment through appropriate channels.

(3) If WAWF is unavailable, manually complete the receiving report with a DD Form 250, "Material Inspection and Receiving Report," and forward a copy to the local Financial Management Accounting Liaison Office for processing to WAWF within three working days of IT asset receipt and acceptance.

c. When managing Capital Assets, DCMA ITAM will work with the Capital Asset Manager, Accounting Specialist, and Component property lead to accurately capitalize and apply depreciation factors to equipment with a unit or system acquisitions cost of $250,000 or more.

(1) When loading the acquisition/lease cost and the fund code, pay particular attention to avoid errors. The Managerial System/APSR 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 DCMA financial statement annually submitted to Congress.

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

d. Common Use Assets. Per DCMA Manual 4401-20, "Position Based Distribution of Information Technology Assets," common use or "shared" equipment (i.e., conference rooms and desk share space such as hoteling stations, shared cubicles and offices, or any area that does not have equipment permanently assigned to a DCMA employee). The allowable standard, per conference room and desk share space, is a monitor and an option for connecting a laptop, keyboard, mouse, and other approved universal serial bus (USB) devices. When the need exceeds the allowable standard equipment, a business case analysis and justification must be submitted through the Agency's intake process. If approved by the Executive Director, DCMAIT, Components will work closely with the local IT staff to determine the most appropriate means to satisfy the requirement. For all special use equipment, the CMO will identify, in writing, the CMO employee who will be the hand receipt holder for it.

## 3.4. ESTABLISHING CUSTODIAL RESPONSIBILITY OF HARDWARE ASSETS.

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

b. 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 safeguarding of the property from causes other than normal wear and tear.

c. There are two methods to establish custodial responsibility.

(1) Establish an organizational asset equipment account in the DCMA Managerial System/APSR. The CIO appoints an IT-APO for the account.

(2) The IT-APO accepts custodial responsibility on behalf of the organization by certifying a Managerial System/APSR inventory list provided by the DAPOs with a handwritten or digital signature.

(a) The DAPO conducts the annual inventory according to Paragraph 3.5.

(b) DAPOs will maintain accountability and tracking of all assigned IT assets. DAPOs will have end users sign a hand receipt or digitally sign an email or system acknowledgment for the hardware assets in the user's possession or hardware assets they use regularly. DAPOs will use hand receipts for easily transported devices such as laptops, PEDs, tablets, portable monitors, etc. Digital signatures are encouraged.

(c) DAPOs will have end users sign a hand receipt, DD Form 1150, for all accountable IT assets in the user's possession or IT assets they use regularly. The first line of the DD Form 1150 will state, "I will not transfer, donate, or otherwise relocate the items listed herein without notification and consent of the DAPO." The DAPO will maintain a copy of the signed hand receipt in DPAS until the user returns the IT assets. Hand receipts will validate equipment location during annual or DAPO-directed inventories. The user will also maintain a copy of the hand receipt as proof of transfer of custodial responsibility to the user. DAPOs may use digital signatures in lieu of wet signatures. Digitally signed emails may be used as proof to re-validate equipment location and status during inventories. Monitors will be considered accountable assets and tracked in the Managerial System/APSR.

(d) Hand receipts may take the form of the DD Form 1150, a digitally signed electronic hand receipt, or a digital signature in an automated system. Users will sign all hand receipts and will provide the signer's contact information. Failure of the End User to sign the hand receipt will result in the denial of services to the agency network. If the DD Form 1150 is not used, the hand receipt or automated system must state:

> "I have received the item(s) listed above on the date indicated. I accept personal responsibility for the property and will surrender it upon demand, transfer, or separation from the Government. I understand that this property is for official use only and that I will comply with US Government, DoD, and DCMA rules, regulations, and guidance concerning the appropriate use and safeguarding of US Government property.
>
> I further understand that failure on my part to exercise responsibility for the care and protection of the items listed above could result in pecuniary liability

established IAW statute, regulation, and policy, including DoDI 5000.64 and DoD 7000.14-R, Volume 12, Chapter 7."

d. IT assets that are components of other major systems and are already tracked in another property management system, will not be tracked in the Managerial System/APSR.

e. Equipment in possession/use of deployed home station personnel will be tracked and managed within the home station inventory. Equipment transferred to other units or left forward must be properly transferred from the home station (losing unit) account to an appropriate gaining unit to maintain full accountability using DD Form 1150, a digitally signed electronic hand receipt, or a digital signature in an automated system.

f. Upon equipment turn-in, a DD Form 1150, a digitally signed electronic hand receipt, or a digital signature in an automated system will be completed to show the completed transfer/turn-in and to ensure the end user is not liable for pecuniary liability for future loss, destruction, or damage to the property.

## 3.5. INVENTORY OF HARDWARE ASSETS.

IAW DoDI 5000.64:

a. An inventory validates the existence, proper location, and correct quantity of hardware assets as stated in the inventory records in the Managerial System/APSR. DAPOs will reconcile inventory with the Managerial System/APSR database records.

b. Official DCMA validation techniques for an inventory include hands-on verification, photo or serial number from the user, barcode scanning, IUID, RFID, and per DoD guidance of June 2021 (DoDI 4140.73), may include network log-on or use records including the Enterprise IT Service Management suite and/or use of network Automated discovery tools (AutoDiscovery).

c. Regardless of the validation technique used during the inventory, DAPOs will reconcile the validation results with the records in the Managerial System/APSR database.

d. DAPOs will conduct the annual inventory by the end of the fiscal year. DAPOs will complete out-of-cycle inventories when directed or required by the IT-APO, IT Director and IT Division Directors, or IT-AM. DAPOs that cannot conduct their annual inventory within this timeframe must submit a written request from the Center/Organizational Director to the DCMA CIO requesting an extension.

e. On completion of the inventory, the DAPO and the IT FS TC or equivalent must approve and certify the official Managerial System/APSR generated inventory with a handwritten or digital signature and forward it to the IT-APO or designated official.

(1) The IT FS TC's signature certifies to the IT-APO that the annual inventory is complete. DAPOs will use this date as the official inventory date in the Managerial System/APSR.

(2) Annual inventories can be certified and completed even if items are missing if the DAPOs document the items as part of an initiated FLIPL investigation.

f. DAPOs will only retain the most current inventory in the IT-APO/DAPO folder or Electronic Records Management system.

(1) The IT-APO will maintain the original certified inventory; a copy will be retained in the DAPO file. DPAS only holds reconciliation documentation for 30 days.

(2) If digital signatures are used, the IT-APO and DAPO will each file a copy in their OneDrive electronic records management system (file plan, electronic records management solution, electronic record-keeping system, or automated information system).

(3) The IT-APO and DAPO will review past inventory records to ensure they are complete before disposing of old inventory data; they will ensure source document retention to support current inventory records (e.g., FLIPL, hand receipts, etc.). Current retention is three years following the End of Life or three years after the Defense Reutilization Marketing Office (DRMO) action.

(4) The DAPO and IT-APO will maintain electronic record folders in DCMA's collaboration environment (O365) with the following suggestions (as applicable) for each tab, directory, or metadata.

(a) TAB 1 – Current digitally signed IT-APO designation.

(b) TAB 2 – Current Annual Inventory.

(c) TAB 3 – DD Form 1150, Hand Receipts (Currently in APS).

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

(e) TAB 5 – Asset transfer documentation (Currently in DPAS).

(f) TAB 6 – Training Certificates.

(5) The format of the tabs will be consistent between the DAPO and IT-APO. They will use automated processes. They will transition existing six-part folders to electronic records management.

g. DAPOs will ensure the Managerial System/APSR inventory listing reflects all assets. DAPOs will determine if work area hardware equipment found that is not on the Managerial

System/APSR inventory listing should be added to the Managerial System/APSR to establish accountability according to guidance from the IT-APO.

h. During the inventory, a DAPO will contact each individual with equipment issued via hand receipt to verify the equipment's status. At a minimum, the DAPO will annotate the following on his/her copy of the hand receipt: person contacted, contact date, updated contact information, if required, and initial the entry. A digitally signed email from the possessor of the equipment is the preferred method of documenting the contact.

i. The IT asset status codes within the Managerial System/APSR will be reviewed during the annual inventory to ensure they reflect the current status. Status codes allow the purchasing agent/entity to make accurate and informed buying decisions. For organizations that centrally procure, these codes are crucial to that process.

j. When completing inventory adjustments in the Managerial System/APSR, DAPOs will use the following database user's manual categories to ensure proper disposition.

(1) Reverse Post.

Reversal of an initial asset addition is permitted only when entries still need to be posted to the official record. Once the DAPO processes a transaction against the record, it cannot be reverse posted.

(2) Maintenance Swap.

Assets returned to the vendor with a replacement asset provided by the vendor.

(3) Returned.

Assets returned to the vendor without replacement.

(4) External Disposal.

This category includes assets disposed outside the normal Managerial System/APSR or DLADS process (e.g., transfer to organization/activities that do not use the Managerial System/APSR to account for IT hardware assets).

(5) Destroyed.

This category includes combat losses, natural disasters, and authorized disposal of IT components in the area of responsibility.

(6) Assets Tracked Elsewhere.

Assets managed by another government system.

(7) Causative Research.

Assets assigned a FLIPL number.

k. During the inventory, if any Managerial System/APSR deficiencies (e.g., missing assets, incorrect locations, unrecorded property items) are identified, DAPOs correct these deficiencies as part of the process.

**3.6. CONTRACTOR GUIDANCE.**

a. Organizational Component Head/Regional Commanders grant contractor employees access to, or allow operation of, government-furnished IT resources or contractor-owned IT resources processing government information. Coordination with the government contracting officer and the company's contract terms and conditions govern access and use.

(1) This Manual and DoDI 5000.64 govern the accountability of all DCMA-owned IT assets furnished to contractors as government-furnished property.

(2) This Manual and DoDI 5000.64 establish the extent of contractor liability in the provisions of the applicable contract's government property clause.

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

c. If contractor support employees are assigned to perform DAPO duties under contract terms, DCMA retains responsibility for obligating funds and receiving assets as they are inherently governmental functions according to Subpart 7.5. of the FAR.

d. The IT-APO functions and responsibilities are defined by DoD FMR 7000.14-R, Volume 12, "Special Accounts, Funds, and Programs," Chapter 7. Accountable Property Officers exercise substantive discretionary authority in determining the US Government's requirements and controlling government assets. The responsibilities of the Accountable Officer and the position of the Accountable Officer are not contractible. The primary accountable officers under the DCMA Accountable Property System include CIO, IT-APO, and IT DAPOs.

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

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

funds. AS THE ACCOUNTABLE OFFICER, the DCMA contractor assigned as alternate DAPO can sign the DD Form 200, block 17.

## 3.7. ACTIVE DUTY GENERAL OR FLAG OFFICER (GFO) AND SENIOR EXECUTIVE SERVICE (SES) CIVILIAN NOTEBOOK COMPUTERS AND PEDS.

a. If the GFO or SES desires, the notebook computer/PED assigned may transfer with the GFO or SES from the DCMA assignment to the DCMA assignment, including devices with a commercial wireless service contract. The GFO or SES will work with the losing and gaining unit to ensure proper inventory accountability. The local DAPO retains accountability for the notebook computer/PED until it is transferred to the new location.

b. When a GFO or SES retires or leaves DCMA service, they must surrender the notebook computer/PED to the supporting DAPO. The surrendered notebook computer/PED data must be preserved or imaged for potential future litigation.

## 3.8. SUPPORT PLANS.

Organizations develop an Acquisitions Strategy, IT Asset Life Cycle Management Plan, and/or Life Cycle Sustainment Plan for IT assets they procure to ensure logistics support throughout the expected lifecycle.

a. A support plan includes planning and developing a spare and repair parts support plan, determining initial requirements, acquisition planning, distribution, and replenishment of inventory spares. A support plan also includes periodic reviews to ensure that IT assets are sustained and upgraded as necessary IAW the target implementation and operational baselines.

b. Although there is no standard method to determine the quantity of spare equipment or repair parts to keep on hand, consider technical data such as mean time between failure rates, reliability data obtained from the manufacturer, and order and ship time from the source of supply when analyzing supply support. Personnel should also consider mission impact factors such as single point of failure and/or mission-critical items. Ultimately, the Agency Director's decision, based on experience with low-density/COTS systems, determines the number of on-hand spares necessary to ensure mission accomplishment.

c. Regardless of the method used to determine the quantity of spare equipment or repair parts to keep on hand, the ITAM manual will capture the rationale/methodology used.

## 3.9. MAINTENANCE MANAGEMENT.

Maintenance management requirements are necessary to avoid risks to personnel, prevent damage to IT equipment, and ensure IT equipment availability to meet the mission.

a. The PM determines if the IT hardware is considered mission-critical or non-mission-critical for maintenance management purposes.

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

c. Cannibalization may be used to satisfy an existing requirement or to meet priority mission requirements if it is the only option available to prevent mission impact. All cannibalization and documentation will be performed according in NIST. SCIF IT hardware assets are excluded from cannibalization actions.

d. DCMAIT Cybersecurity Center approval is required before initiating any cannibalization action on mission-critical IT equipment.

e. The PM (or equivalent) or designated representative can approve cannibalizing operational non-mission-critical IT equipment.

f. The local IT Division Director (or equivalent) may also approve using unserviceable IT hardware assets as a source for spare parts to maintain other IT equipment. An explicit cost analysis indicating the economic feasibility of using excess assets versus procuring new items determines the use of this authority.

g. Assemblies, sub-assemblies, and parts obtained for maintenance redundancy or operational spares are accounted for in the Managerial System/APSR. Ensure the IT asset status in the Managerial System/APSR is updated to identify these items as operational spares.

h. Before the IT assets disposition, verify that warranty dates and asset recovery statuses are outside their warranty expiration or subject to asset recovery rules.

## 3.10. IT SYSTEMS MAINTENANCE REPORTING.

Users with maintenance contracts document all IT asset maintenance on vendor maintenance forms according to the appropriate/applicable contract.

## 3.11. COMPUTATION OF PAYMENTS.

Computation of payments for hardware assets, purchased or leased, will clearly state the effective start date.

a. Contracts that apply to managed hardware assets will clearly state the effective start date. A lease document will clearly state the effective date for rented/leased IT assets. 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.

b. Computed charges for rented/leased IT assets will be reported to the DAPOs by the contract or lease PMs using available vendor forms.

c. For DCMA-managed systems, the verifying activity refers to the equipment utilization reports and the input to the reports (IT assets/equipment orders and other appropriate records) to validate the services. Claims will be submitted for credit within 60 calendar days (or as stated in the contract). The IT asset contract manager/PM/IT-APO designates the verifying activity for non-DCMA managed systems (e.g., joint service systems).

## 3.12. GUIDANCE FOR TRANSFER OR DISPOSITION OF HARDWARE ASSETS.

a. The DAPO will clear all UIC assets before closing the account (closures, mission changes, etc.). The DAPO (or equivalent) remains accountable for all assets until properly closed.

b. The DAPO will ensure the disposition of DoD computer hard drives and/or hard drive sanitization is performed IAW NIST SP 800-88 R1. IT assets within SCIFs will follow the Intelligence Community Directive 503, Committee on National Security Systems Instruction 1253 or other policies issued by national IC elements.

c. The DAPO will ensure disposal and destruction of classified hard drives, electronic media, processing equipment components, and the like is accomplished IAW DoDM 5200.01, Volume 3, and the NSA/CSS Policy Manual 9-12, "Storage Device Sanitization and Destruction Manual" utilizing equipment listed on the NSA EPL. For Controlled Cryptographic Items, reference, NSA/CSS POLICY 6-22**, "**Handling of NSA/CSS Information Storage Media.

d. The DAPO will ensure disposal of Controlled Unclassified Information and unclassified electronic media is accomplished IAW the guidelines provided in NIST SP 800-88, Rev. 1 and applicable security controls.

e. Software purchased with the original equipment manufacturer is considered an integral part of the system. Therefore, the software must be maintained with the system. If the system is transferred, the software licenses must accompany the system. The DAPO will ensure the transfer of all software licenses with the system. An exception may be when the terms of the software license allow for software to be recoverable and reused upon decommissioning of system assets.

## 3.13. TRANSFERRING NON-EXCESS HARDWARE ASSETS TO ANOTHER DOD COMPONENT, FEDERAL AGENCY, STATE, OR LOCAL GOVERNMENT.

The transfer of non-excess IT assets occurs when a function (e.g., base realignment and closure) and the IT assets acquired to support that function are transferred to another DoD component or federal agency. DAPO's must ensure their organization is included in the Memorandum of Agreement (MOA) between DCMA and DLA.

a. The losing DAPO provides the IT-APO with a letter of transfer (DD1150), signed by the losing DAPO, documenting the transfer of the function and equipment.

b. 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 DAPO. The gaining and losing DAPOs sign the DD Form 1149 for local transfers where no shipping activity is involved.

c. The losing activity DAPO will account for the transferred hardware. The DAPO will also identify excess hardware created due to the transfer of a function.

(1) The DAPO and the gaining DAPO or other accountable officer will identify and report maintenance contracts that support transferred assets to contracting officials.

(2) The losing DAPO will:

(a) Update the Managerial System/APSR asset status field using approved codes.

(b) Provide account records information to the gaining activity as required.

(c) Review all contract obligations with the gaining and losing activities and contracting officials. Pay close attention to any contract termination clauses (applies when the losing organization has paid for extra maintenance). Use the currently established Managerial System/APSR guidance to remove items from an account.

(d) Review hardware assets release dates. Give the PM adequate notice so they can notify the vendor to preclude payment of extra costs.

(e) Coordinate hardware assets release dates with other agency functions, as required.

(f) Ensure hard drive sanitization is IAW DCMA-MAN 3301-08, DoDM 5200.01, Volume 3, DoDI 5200.48, NSA/CSS Policy Manual 9-12, "Storage Device Sanitization and Destruction Manual" utilizing equipment listed on the NSA EPL, and NIST SP 800-88, Rev. 1, as applicable.

(g) Provide the hardware system database records or custodian report to the IT-APO. The IT-APO will add all applicable records regarding the transfer to their applicable IT-APO electronic records.

(h) Properly inventory, package, warehouse, and secure equipment when storing hardware assets before transfer.

## 3.14. EXCESS HARDWARE.

Mission change, equipment upgrades, technology changes, out-of-warranty status, obsolescence, etc., determine if an item is excess. 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. Accountable individuals are responsible for

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

a. If applicable, DAPOs will use the Excess IT Hardware Assets form to report serviceable spares older than five years.

b. The DAPO will change the asset's status code to 41 (Discontinued use) if older, unused inventory remains in DPAS.

## 3.15. OBTAINING EXCESS RESOURCES.

a. The PM or DAPO may direct hardware asset reutilization for new requirements or to replace equipment that does not meet minimum standards.

b. To acquire equipment from DLADS, the DAPO submits documentation (DD Form 1348-1A) for coordination with the DLADS. The DAPO can view assets at the DLADS location or research at the DLADS site. Both links are available on the resource page.

c. DAPOs establish accountability in the Managerial System/APSR for hardware equipment acquired through any source that meets the criteria for accountability IAW this manual.

## 3.16. TRANSFERRING EXCESS HARDWARE ASSETS TO THE DLADS.

a. Asset Recovery or DLADS is the primary DoD process for the disposal of all obsolete, unserviceable, or excess military property and equipment. Use these processes to dispose of all DCMA hardware.

b. The DLADS site contains guidelines for the disposition of excess hardware assets, including disposal. The resource page has the site link.

c. All media being disposed of or transferred to DLADS or another entity outside of the DoD will be sanitized and/or destroyed as applicable according to DCMA-MAN 3301-08, DoDM 5200.01, Volume 3, DoDI 5200.48, NSA/CSS Policy Manual 9-12, "Storage Device Sanitization and Destruction Manual" utilizing equipment listed on the NSA EPL, and NIST SP 800-88, R1, as applicable.

d. DAPOs must establish a MOA with their servicing DLADS office to transfer IT equipment directly to local schools under the Computers for Learning Program. Donations of IT equipment to schools can only occur AFTER completion of the mandatory DoD reutilization screening, and then IT equipment donations can only be to registered and qualified institutions identified by the DLADS.

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

f. DAPOs will use the Managerial System/APSR-generated DCMA APS Form to process DLADS disposals. (DAPOs may also use the equivalent DoD form, DD Form 1150.) DAPOs may not use an electronic turn-in document for these transactions.

## 3.17. ASSET RECOVERY, EXCHANGE, OR SALE OF GOVERNMENT AUTOMATED RESOURCES.

a. Contract partners have programs designed to recover (e.g., give credit for equipment that still has market value) or recycle (e.g., dispose of hardware assets in an environmentally safe manner and replace due to obsolescence or un-serviceability) hardware assets. The proceeds or credit are applied toward purchasing replacement government automation resources. (See DoDM 4140.01, Volume 12, and Defense Federal Acquisition Regulation Supplement (DFARS), current edition, Part 217.70, "Exchange of Personal Property," for more specific guidance)

b. Adhere to disposal procedures IAW DCMA-MAN 3301-08, DoDM 5200.01, Volume 3, DoDI 5200.48, NSA/CSS Policy Manual 9-12, "Storage Device Sanitization and Destruction Manual" utilizing equipment listed on the NSA EPL, and NIST SP 800-88, R1, as applicable.

## 3.18. ASSET DISPOSITIONING PROCESS PERTAINING TO DCMAS SPECIAL PROGRAMS.

DCMAS hardware asset management dispositioning policy is outside the scope of this Manual but will be contained in DoDM 5205.07, Volume 1.

# SECTION 4: SAM

## 4.1. SOFTWARE ASSETS GENERAL GUIDANCE AND PROCEDURES.

SAM will be centralized and managed at the DCMAIT Directorate level. The CIO implements licensed COTS or other software for local requirements, including those software licenses managed through enterprise software licensing programs. The DCMA SAM program ensures that the Agency deploys, manages, and tracks COTS software entitlements and implementation information.

a. DCMA ITAM or SAM designee will maintain a hard or soft copy of the software license inventory and "Proof-of-License Ownership" of GOTS/COTS software in use within the Agency.

b. DCMA ITAM or SAM designee will store proof of license agreements or licenses (e.g., user manuals, purchase documentation, compact disks, etc.) and software media in a secure, centralized location (e.g., locked drawer, file cabinet, room, etc.) or electronically if applicable.

c. DCMA ITAM or SAM designee will inventory all licensed software annually and, if available, use AutoDiscovery to track and report implemented software and license information.

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

(2) Place semi-annual reminders of the need for proper software license management in DCMA Messenger and other media to increase and reinforce the legal requirement of maintaining software licenses according to their stated conditions.

d. Redistribute excess or superseded software if it:

(1) Is permitted under the license agreement or upgrade policy for that software.

(2) Is not classified.

(3) Did not provide direct security protection to systems that processed classified information.

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

(5) Still operates as intended.

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

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

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

f. The organization Control:

(1) Uses software and associated documentation IAW contract agreements and copyright laws.

(2) Tracks the inventory, software usage, and associated documentation protected by quantity licenses to control copying and distribution.

(3) Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. Software license tracking can be accomplished by manual methods (e.g., Supplemental Guidance: simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.

## 4.2. ORDERING AND/OR PROCURING SOFTWARE.

a. All DCMA software will be procured using applicable DoD enterprise buying programs.

(1) Joint or DoD ELAs authorized for DCMA use and DoD ESI/SmartBuy are the primary sources for software purchases.

(2) Any software product, maintenance, and related hardware or services not offered by an ELA or DoD ESI must be procured using DCMA or DITCO Contract.

b. All software used on DCMA networks must be evaluated and certified/assessed by the appropriate Cyber Security or DISA equivalent office. The list of evaluated products is on the resource page.

c. All requests for server software must comply with the National Defense Authorization Act, and a DoD Unique identifying number must accompany the acquisition.

d. All software purchases will comply with Sections 2222 of Title 10, U.S.C., and the most recent published guidance for Defense Business Systems Funds Certification and Defense Business System Integrated Program/Budget Review (currently, Version 3.0 published April 2014).

## 4.3. SOFTWARE DEVELOPED USING COTS TOOLS.

All DCMA personnel will use licensed COTS office software to increase productivity and overall Agency effectiveness. Users may develop shared single-user, networked multi-user, or

"group" computer applications built with COTS office software tools. Applications built by citizen developers will abide by the same rules (build, test, deploy) as other agency commercial applications. This process ensures that the impact on network and server capacity is accounted for and provides continued software support after one or more of the original user developers depart. DCMA software developers will:

a. Ensure DCMA retains property rights to the computer software developed in the course of their duties.

b. Not bypass computer and network server operating systems, security systems, or access controls from higher authority.

c. Provide DCMA a software documentation package in an appropriate digital format. The software package must include:

(1) The author or point of contact, organization, and telephone number.

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

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

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

(5) A brief user's guide. The user's guide should include:

(a) The hardware configuration required.

(b) The supporting software required, including the operating system and any supporting COTS software with version release number.

(c) Compiling and linking instructions, if applicable.

(d) Descriptions of the software installation process, required hardware setup, menus, and software capabilities and functions.

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

(f) Other helpful information for continued effective use and maintenance of the mission application software.

## 4.4. COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, AND INTELLIGENCE SOFTWARE DEVELOPMENT, REUSE, AND RELEASE.

Adhere to DoDI 8330.01 and the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems" when developing mission or application software for Command, Control, Communications, Computers, and Intelligence systems.

### a. Organic Software Development.

Only develop software organically if quality, cost, performance, schedule, or interoperability requirements cannot be met with COTS or non-developmental item software. Develop requirements for IT capabilities IAW the National Defense Authorization Act of 2014, Section 937.

(1) Acquire an approved mission needs statement before developing organic software requiring over six person-months of effort or costing over $50,000. The contract must contain the proper FAR/DFAR clauses on data rights if a contractor develops the software organically.

(2) IT Divisions that develop or maintain software code will have a Software Process Improvement (SPI) program and a documented SPI plan that, at a minimum, includes:

(a) A baseline of their current capabilities.

(b) Goals and milestones they intend to reach.

(c) Metrics to measure their progress toward their goals and milestones.

(d) Timeline for SPI appraisals: Identify life-cycle support requirements for the life of developed software.

### b. Government Software Release or Disclosure.

It is agency practice, IAW DoDI 5000-87, to release, upon consideration of a valid written request, specific software developed with government funds, which is a government work (created by government personnel), or software created by a contractor where DCMA has a government rights license. Release of software by DCMA is not permitted if it violates a copyright or terms of a contract. The CIO, or designated alternate, is the approval authority to release or disclose software.

(1) Before releasing software, the OPR will require the requester to sign an MOA. The MOA will include how to govern maintenance and support relationships for the software or document the lack of these relationships if the OPR does not provide support.

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

(3) Using the Software Engineering Institute's Software Capability Maturity Model Integrated, or the Systems Engineering Process, is desirable when developing mission or application software for information systems.

## 4.5. SOFTWARE CONFIGURATION, CHANGE, AND RELEASE MANAGEMENT.

Use IT Configuration Management and Change Management Services for Configuration Management and Change Management as applicable. Use ISO/IEC 20000, or Information Technology Infrastructure Library, Configuration Management, Change Management, and Release Management processes to plan, identify, control, monitor, verify, and manage software configuration items. Typically, software configuration items include information such as purchase order number, purchase date, software manufacturer, software title, and version implemented.

a. A single software management system will be used for software and software license configuration or change management as needed.

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

(1) Adhere to the guidance given in the DoD Information Enterprise Architecture. The link is on the resource page.

(2) Ensure that upgrades to systems under maintenance comply to the maximum extent possible with the DoD Information Enterprise Architecture and DCMA baselines as they are updated.

c. DCMA is committed to sharing DCMA information with those with a valid need. To that end, architectural artifacts must capture the roles and permissions of users of DCMA information in the context of the supported mission and business processes. The authorization and access provisioning to that information should support the defined roles and permissions.

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

(1) Reusable software components may include executable software binaries, source code segments, program documentation, project plans, requirement descriptions, design and

architecture documents, database schemas, test data and test plans, user's manuals, software tools, and object classes.

(a) These assets are most efficiently reused when designed to fit into a product-line architecture for a mission area or functional domain using standard interfaces and common communications protocols, including 508.

(b) Domain product-line components can be used to create families of related systems that share a common software architecture for the domain.

(2) DCMAIT maintains a software reuse library or repository for internal sharing of the reusable software components developed at DCMA (e.g., MOCAS).

e. DCMA is faced with restrictions on how much information can be provided to its users. Therefore, software designers and developers must discipline themselves in the quantity and content of non-mission essential information sent over supporting network infrastructures (i.e., ensuring sending only operationally necessary data).

(1) In addition to DoD direction, follow all policies and procedures on downloading from the Internet, transmission of email attachments, video teleconferencing, Web browsing, and conservation measures during periods of surge or network degradation.

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

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

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

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

(3) Be clientless with all web services and applications accessible securely via standard web browsers from DCMA standard desktops or other edge devices.

(4) Use strong two-way authentication using public key infrastructure when available.

(5) Fund software development IAW DoD 7000.14-R Volume 4, Chapter 27, Table 27-1, Financial Management Regulation.

# SECTION 5: SOFTWARE AND HARDWARE CONTRACTS

## 5.1. SOFTWARE AND HARDWARE CONTRACTS.

Software and hardware contracts establish the entitlements a publisher or manufacturer provides to the end users in DCMA. Software and hardware contracts will be centralized and managed at the DCMAIT Directorate level. The DCMA SAM program ensures the Agency deploys, manages, and tracks COTS software and hardware entitlements and implementation information.

## 5.2. CONTRACT REQUIREMENTS.

a. All Software and Hardware contracts will include the DCMAIT Asset Management email distribution address as part of the contract package preparation. This information is on the resource page.

b. All contracts will contain alternate WAWF Point of Contact of the DCMAIT Asset Management email distribution. This information is on the resource page.

c. All PMs of a software or hardware package will validate their contract audit plan and lifecycle management plan with the ITAM office.

d. All software and hardware contract packages, including annual option renewals and those processed using simplified acquisition or government purchase card method, will include a current year requirement information memo clearly stating and validating the requirement.

# SECTION 6: IUS

## 6.1. IUS.

a. Capital IUS is included as General Property, Plant and Equipment (PP&E), on the Balance Sheet and represents the costs of software, whether COTS, internally developed or contractor developed, that meet the DoD capitalization threshold and criteria, as follows:

(1) Has an estimated useful life of two years or more.

(2) Not intended for sale in the ordinary course of operations.

(3) Acquired or constructed to be used or available for use by the entity.

b. IUS includes application and operating system programs, procedures, rules, and any associated documentation on the operation of a computer system or program used for operational or other internal use. Normally, the software is an integral part of an overall system having interrelationships between software, hardware, personnel, procedures, controls, and data. It is a stand-alone application, or the combined software components of an IT system, that can consist of multiple applications, modules, or other software components integrated and used to fulfill the entity's internal or operational needs (software type).

c. DCMA ITAM will include all costs that meet the capitalization threshold and criteria for IUS, such as acquisition costs; all costs to bring the software into service (e.g., contractor costs, installation, implementation cost, programming costs, direct and indirect costs, overhead costs); qualifying program management costs; costs to make any enhancement or modification to existing IUS that significantly increases functionality and adds new capabilities (which exceeds the capitalization threshold independently); contractor-developed and internally developed software costs (software development stage); and any qualifying software in development costs. Also, include any IUS capital leases and bulk purchases that meet the DoD capitalization threshold and criteria.

d. Depending on the situation, some preliminary design and post-implementation costs and data conversion costs incurred may need to be expensed. IUS costs may include computer software integrated into and necessary to operate general PP&E rather than perform an application. This software will be considered part of the PP&E, which is an integral part and capitalized and depreciated accordingly. Also, any research, development, test, and evaluation costs, unless the costs are associated with developing an end item produced for operational use and placed in service, may be expensed.

## 6.2. CAPITALIZATION THRESHOLDS.

Include all qualifying costs to determine if an asset meets the threshold:

a. $250,000 and above for acquisitions and modifications/improvements accepted and placed into service October 1, 2013, and after.

b. $100,000 and above for acquisitions and modifications/improvements placed into service prior to October 1, 2013. (See DoD FMR 7000.14-R)

**6.3. BUDGET STAKEHOLDERS.**

a. DCMA DAI Inquiry.

Responsibility within DAI contains the depicted inquiry-only roles.

b. Budget to Reporting Inquiry allows users to inquire on journals and account balances, including sub-ledger details.

c. DCMA Budget Analyst responsibility allows users to enter and maintain appropriations and distribute funds. It also provides access to inquiry functions included in the Inquiry responsibility.

d. DCMA Budget Manager access includes access to all Budget Analyst roles and some additional roles.

e. DFAS manages the values that comprise the line(s) of accounting or chart of accounts. DAI supports a standard, shared accounting line based on the Standard Financial Information Structure and the United States Standard General Ledger. This common line of accounting structure and the related data elements are reported or associated with every transaction users enter or interface into DAI.

f. Budget Stakeholder Responsibility Table 2 is on the resource page of this Manual.

**6.4. APSR.**

a. DPAS is a DoD property management system. It is the APSR for DCMA. DPAS is a fully compliant and auditable APSR.

b. An essential aspect of APSRs/DPAS accountable property records are the data elements required to make a comprehensive record. DoDI 5000.64 outlines these requirements, which include the:

(1) Name of the asset.

(2) Unique Item Identifier (UII).

(3) Stock number.

(4) Acquisition cost or full cost value.

(5) Location.

(6) Status.

(7) Other essential elements.

c. Go to DoD Office of the Under Secretary of Defense Acquisitions, Technology, & Logistics – Property & Equipment Policy under Guidance on the resource page for this manual.

## 6.5. DPAS KEY STAKEHOLDERS.

a**.** The APO is most often in charge of asset management for the Agency and may also have limited policy-setting duties. The user has the highest functional level of access to DPAS. A government employee will fill this inherently governmental role and be designated in writing. The user can perform functions needed to set up Web DPAS for the entire Agency. This role must not have any security access. This role also has equal access to both Accountable and Non-Accountable Property.

b. The PA is the highest level of support to the APO and is considered the designated representative of the APO to support administrative work. A contractor can fill this supporting role. This role does not have security access, nor does it have any Catalog or Manufacturer functions. The PA has equal access to both accountable and non-accountable property.

c. The Accounting Specialist performs finance and accounting functions only for the corresponding asset management system. The Accounting Specialist also performs the Attestation Role quarterly or annually to verify facts and finances about Construction in Progress projects, those completed or those in progress, and personnel and assets involved.

d. Other Responsible Positions include: Asset Receiver, Asset Disposition, Asset Transfer, Inventory Specialist, Custodian, Catalog Manager, Automated Inventory Technician, Accountable Update, Data Inquiry, Report and Forms Generation, Agency Coordinator, Stock Number Authorizations, and Maintenance & Utilization Setup.

## 6.6. DPAS INSTRUCTIONS.

Links to all procedures are on the resource page in this Manual. To fulfill the requirements for Property Accountability, DCMA APOs will use DPAS to:

a. Calculate and transmit accounting transactions to the Financial Accounting Systems (DAI/ Oracle);

b. Integrate with the DAI/Oracle system to provide:

(1) New Receipts to be received from DAI.

(2) Asset Transfers from DoD Organizations.

(3) Asset Transfers to Contractors as Government Furnished Property (GFP).

(4) Asset Transfers from Contractors to return GFP.

c. Manage Software Licenses and the assets the software is installed.

d. Integrated with the IUID Registry to update all Life Cycle events for assets.

e. RFID tagging and reading capabilities to include the ability to use Real Time Location System to locate and map assets.

f. Use of Hand-Held Devices to perform inventories, asset relocation, and UII Associations.

g. DPAS Instructions

(1) Site Setup.

(2) Transactional Setup.

(3) Customization.

(4) Catalog.

(5) Asset Receiving.

(6) Asset Updates.

(7) Asset Transfers.

(8) Asset Disposition.

(9) Inventory Prep and Management.

(10) Inventories.

(11) Conducting an Inventory.

(12) Depreciation.

(13) Construction in Progress.

(14) Real Property.

(15) Improvements and Ancillary.

(16) Inquiries.

(17) Reports and Forms.

(18) Authorizations.

(19) Attestation.

(20) Warranty and Utilization.

(21) Maintenance & Utilization Setup.

(22) IT Management.

## 6.7. KEY SUPPORTING DOCUMENTATION TO SUPPORT ALL BUSINESS PROCESSES AND SUB-PROCESSES ASSOCIATED WITH IUS, INCLUDING ACQUISITIONS, AMORTIZATION, TRANSFERS, AND DISPOSITIONS:

a. Create IUS Project (capital or non-capital) in DAI.

b. Detailed asset lists and summary schedules (reporting amounts/quantities by class of assets).

c. Contract documentation, including (for base assets and asset modifications):

(1) SOW.

(2) Contract clauses that define who owns assets and when the reporting entity takes possession; Purchase Orders.

(3) Receiving report or other acceptance document (e.g., DD Form 250).

d. Obligating documents supporting asset acquisition and any related asset improvements, such as contracts/SOWs, work orders, reimbursable agreements, Military Interdepartmental Purchase Request (MIPRs), purchase orders, receiving reports and invoices, and appraisal reports for donated assets - must demonstrate how a modification increases functionality and the estimated useful life of the asset.

(1) Documentation supporting any retirements, transfers, sales, or other disposal of idle, excess, obsolete, or otherwise unusable assets such as:

(a) Request for Transfer of Excess Real and Related Personal Property (GSA Form 1334).

(b) Declaration of Excess document.

(c) Approval documentation; documents supporting disposal start date.

(d) Documents supporting the determination of impairment from the performance of physical asset/inventory counts.

(2) DD Form 1150 – Request for Issue/Transfer/Turn-In.

(3) Documentation supporting the "placed-in-service" date (e.g., DD 1354, "Transfer and Acceptance of Real Property," DD Form 250, "Material Inspection and Receiving Report," receiving report), including documentation supporting the valid life estimate for recognition of depreciation/amortization expense.

# SECTION 7: ANNUAL PHYSICAL INVENTORY

## 7.1. ANNUAL PHYSICAL INVENTORY.

An annual 100 percent physical inventory is completed by the Property Custodian (PC)/Hand Receipt Holder (HRH) using automated barcode technology (for those assets with barcodes) and manually using inventory checklists (for those assets without barcodes). RMIC control point: verification of DPAS inventory status code (technical control).

a. DCMA will perform periodic physical inventories of PP&E IAW DoDI 5000.64 for tangible equipment.

b. Physical inventory plans will provide a schedule for completing all physical inventories and must include an awareness of an item's acquisition or replacement cost, security classification, and criticality. Physical inventory plans shall provide a schedule for completion of all physical inventories and must include an awareness of an item's acquisition or replacement cost, security classification, and its criticality. At a minimum, property shall be inventoried at least every three years; classified or sensitive property shall be inventoried at least annually. If inventories reveal Critical Information IAW DCMA-MAN 3301-06, "Operations Security," then ensure the inventory plans are marked as "CUI" IAW DoDI 5200.48.

## 7.2. RECONCILIATION.

Inventory/location data is uploaded directly from the scanner into the DPAS or manually input from the inventory checklists. RMIC control point: reconciliation must be completed to close out inventory (technical control).

**a. Discrepant asset processing.**

DPAS automatically produces discrepancies, identifying overages, shortages, and location changes. Resolve all discrepancies to complete the DPAS inventory. RMIC control point: DPAS inventory close-out status (technical control).

**b. Signature page.**

At close out of the inventory, the PC/HRH certifies completion of the inventory with signature.

**c. RMIC Control point.**

PC/HRH maintains certification documents; APOs review (administrative control and accountability) IAW:

(1) DoD 7000.14-R, Volume 4, Chapter 6.

(2) DoDI 5000.64

(3) DCMAIT Asset Management Process & Internal Controls.

## 7.3. PHYSICAL INVENTORY STAKEHOLDERS.

a. DCMAIT Primary APO.

b. Individual APOs are assigned to each geographical DCMAIT Field Services Region.

c. PCs/UIC HRHs.

d. Property Sub-HRHs.

e. COR

f. Management Analysts.

# SECTION 8: ENTERPRISE ADP EQUIPMENT

## 8.1. PROCUREMENT OF IT ADP EQUIPMENT.

Reference DCMA-MAN 4101-04, "Accountable Property & General Equipment," Section 4.

## 8.2. BUDGET PROCESS.

Reference DCMA-MAN 4101-04, Section 2.

## 8.3. PROPERTY ACQUISITION & MANAGEMENT, DISPOSAL OF EQUIPMENT AND PROPERTY LOSS.

a. Reference DCMA-MAN 4101-04, Section 4.

b. Reference DCMA-MAN 4101-04, Section 5.

c. Reference DCMA-MAN 4101-04, Section 6.

## 8.4. DCMA BUDGET ANALYST.

The DCMA Budget Analyst responsibility allows users to enter and maintain appropriations and distribute funds.

## 8.5. FIELD SERVICES CENTER PROCESSES.

### a. APO-IT will assign PAs for each UIC in IT.

The PA will assign PCs/UIC HRHs for specific UICs. PAs are responsible for the day-to-day equipment management, including receipt, distribution, tracking, disposal, annual physical inventories, and reconciliations.

### b. Property Sub-HRH.

DCMA customers are assigned as property sub-HRHs at distribution of individual equipment.

### c. PM.

DCMAIT assigns individual Program or Project Managers for each procurement action, (e.g., laptops, USB hard drives, and workstations). The PMs are responsible for the annual establishment of life cycle management procedures for their assigned procurement actions, including receipt and disposal of legacy equipment. Inclusive of this responsibility, the PMs coordinate with the vendor and receiver to ensure that assets procured, shipped, and received are documented accordingly (i.e., the serial numbers and quantities match).

**d. Management Analysts.**

DCMAIT employs management analysts to assist with data entry, asset transfers/disposals, and annual inventories.

**e. Receipt.**

Assets are physically received and inspected by authorized individuals identified in the Advance Shipment Notice. DAPOs accept receipts from authorized personnel.

**f. Storage.**

Assets not used during daily operations are stored in a secured area with documented and limited access. Facility security and or IT personnel review and spot-check locked storage areas.

**g. Disposition.**

Assets dispositioned are properly documented and signed for and then removed from ADP systems (Managerial System/APSR). Turn-in documents are reviewed against dispositioned assets.

## 8.6. INTERNAL CONTROLS.

**a. Receipt.**

Verification of receipt, including quantities and serial numbers, is performed at three levels of the organization: COR, Local Area Administrators (LAN Admins), PC/HRH, and APO. The IT-APO initiates a mass data entry input into the property accountability system, verified by the local LAN ADMINs and re-verified by the COR at completion. At each level of the process, segregated roles verify the accuracy of data and quantities.

**b. Documentation.**

The local APO/PA verifies data input into the DPAS. The customer confirms the serial numbers of the asset and certifies receipt of the equipment by signing the hand receipt and sending it to APO/PA to be attached in DPAS to the assets.

**c. Inventory.**

Using multiple LAN ADMINs (i.e., Tiger Teams) and the local PC/HRH during the physical inventory process reduces the risk of fraudulent transactions. Barcode scanner data, when processed, detects overage and or shortages and automatically detects assets scanned in a different UIC (a/t/o control).

**d. Established Procedures.**

Routine procedures followed at each control point (receipt, mass upload, asset deployment, transfers, and disposition) ensure PC/HRHs and APOs complete all transactions. Asynchronous transactions identify discrepancies at multiple points along the Lifecycle Management (LCM) process (a/o control).

**e. Physical Control.**

The APO appoints the AP to maintain positive asset control throughout the LCM process. The receiving PC/HRH or local LAN ADMIN confirms inspection reports in WAWF; only authorized personnel confirm inspection reports. The Facility's physical security personnel maintain appropriate locks and access control lists. Changes in access control lists are only authorized at the APO level.

**f. Oversight.**

Automated systems and weekly roll-up reporting requirements maintain continuous process oversight at the COR, APO, Division, and Directorate levels. COR/APO reporting data (quantities) are verified throughout all points in the process (e.g., receipt, configuration, distribution).

## 8.7. ADP SYSTEMS.

DCMAIT uses relational key fields, both primary and foreign, within its ADP systems to verify and analyze data accuracy and quantities across the enterprise spectrum.

**a. Asset/Financial Management Systems.**

(1) DPAS – DCMAIT official property accountability system.

(a) UIC.

Groups assets together under the responsibility of an individual PC/HRH and APO. It is cross-referenced in the procurement and mass upload processes.

(b) Site Identification (ID).

Asset physical identification locator. Used to group, procure, deliver, and mass upload asset quantities.

(c) Serial Number.

Unique asset identifier provided by vendor/manufacturer. Cross-referenced in WAWF, process checklists/worksheets, and Managerial System/APSR.

(d) Asset ID.

Unique asset identifier produced by DCMA IT-APO during mass upload to DPAS.

(e) Property Description.

Identifies the year of procurement. Cross-referenced in contracting documents, LCM process checklists in DPAS.

(2) DPAS – DCMAIT official sub-hand receipt system.

(a) Serial Number.

Unique asset identifier provided by vendor/manufacturer. Cross-referenced in WAWF, Invoicing, Receipt, Acceptance, and Property Transfer (iRapt), LCM process checklists/worksheets, the Managerial System/APSR, and Tivoli Enterprise Management System (TEM).

(b) Barcode (Cage Code, Serial Number, Part Number).

Unique asset identifier produced by DCMA IT-APO during mass upload to DPAS.

(c) Issued To.

Sub-HRH. Identifies current owner/user of the asset.

(d) Issued By.

Identifies PC/HRH or local LAN ADMIN issuing equipment. Cross-referenced in LCM process checklists/worksheets, DPAS and Lan Admin Locator (LAL).

(e) Computer Name.

Identifies hostname of asset and/or physical location of the asset. Cross-referenced in LCM process checklists/worksheets, and Active Directory (AD).

(f) Property Description.

Identifies the year of procurement. Cross-referenced in contracting documents, LCM process checklists/worksheets, and the Managerial System/APSR.

(3) WAWF – Used to validate receipt and authorize payment to the vendor.

(a) Serial Number.

Unique asset identifier provided by vendor/manufacturer. Cross-referenced in WAWF, LCM process checklists/worksheets, the Managerial System/APSR, and TEM.

(b) Quantities.

Cross-referenced in LCM process checklists/worksheets, the Managerial System/APSR.

**b. Enterprise Architecture Systems.**

(1) TEM.

The enterprise management system used throughout DCMAIT for management control of the enterprise (technical control).

(a) Serial Number.

Unique asset identifier provided by vendor/manufacturer. Cross-referenced in WAWF, LCM process checklists/worksheets, the Managerial System/APSR, TEM, and Magic.

(b) Computer Name.

In conjunction with the DCMAIT standard naming convention, it identifies the year of procurement, model, and physical location. It is cross-referenced in DPAS, LAL, LCM process checklists/worksheets, the Managerial System/APSR, TEM, and AD.

(c) IP number.

Identifies the physical network location of the asset. It is cross-referenced in LAL, LCM process checklists/worksheets, and the Managerial System/APSR.

(d) Last User ID.

Identifies the last customer to operate the asset. It is cross-referenced in the Managerial System/APSR and AD.

(2) AD.

Enterprise management system used throughout DCMAIT for management control of the enterprise (technical control).

(a) Computer Name.

In conjunction with the DCMAIT standard naming convention, it identifies the year of procurement, model, and physical location. It is cross-referenced in DPAS, LCM process checklists, and TEM.

(b) Description.

Identifies the current operator of the asset. It is cross-referenced in DPAS.

(3) SunView ChangeGear Service Center Database.

Service Center software/database used to manage all service/warranty requests/issues (technical control).

(a) Computer Name.

In conjunction with the DCMAIT standard naming convention, it identifies the year of procurement, model, and physical location. It is cross-referenced in DPAS, LAL, LCM process checklists/worksheets, and TEM.

(b) Incident Description.

Used to record the serial number of all assets submitted for warranty repair/replacement. The serial number is cross-referenced in WAWF, LCM process checklists/worksheets, and the Managerial System/APSR.

(c) Customer User ID.

It records the customer's name. In conjunction with warranty repairs, the User ID is cross-referenced with the computer name in AD, LCM process checklists/worksheets, and the Managerial System/APSR and TEM.

(4) LAN ADMIN Locator (LAL).

The enterprise management system used throughout DCMAIT for administrative control of the enterprise (administrative control). The Site ID is the Physical ID locator of individual Agency sites. It is cross-referenced in LCM process checklists/worksheets.

**c. Internal Controls.**

(1) Appointment letters.

Appointment letters, initiated by the IT-APO, identify roles and responsibilities.

(2) Control Environment.

DCMAIT uses ADP systems in conjunction with daily operations; utilization of systems is mandatory in performing DCMAIT duties and responsibilities. The operation of the DCMAIT Enterprise Architecture is layered both laterally and vertically; failure to meet specific tasks is identified throughout the organization, (e.g., security and operations.)

(3) Integrated systems.

The utilization of multi-tiered ADP systems with primary/foreign keys provides reasonable assurances of cross-reference capabilities.

(4) Discrepant quantities or serial numbers.

Discrepant quantities or serial numbers are cross-referenced in multiple ADP systems.

(5) Add Subtitle here since (1)-(4) have one.

Management/technical personnel (CORs, APOs, Division/Center Director levels) receive/produce an integrated set of standard reports and forms and apply metrics and performance measures to consistently monitor standard processes against objectives.

**d. Standard Reports/Forms.**

(1) Reconciliation.

Automated DPAS report to identify overages/shortages during the inventory process. Reconciliation of overages/shortages will be completed to produce a DPAS status change of inventory report.

(2) DPAS.

Produced by DPAS at the completion of the inventory. PC/HRH maintains signed certification forms for each physical inventory; APO reviews the document.

(3) DD Form 200, "Financial Liability Investigation of Property Loss."

Document to record/report the suspected loss and is initiated by the sub-HRH or PC/HRH. DD Form 200 requires the signature of the IT-APO, Division Chief, and Center Director before the deletion of assets from DPAS. Attach the form in DPAS after all signatures are captured.

(4) DD From 362, "Statement of Charges/Cash Collection Voucher."

Document the expense associated with the buying of certain stock or goods. Also referred to as Statement of Charges.

(5) DD Form 1348, "Issue Release Document."

Automated turn-in document produced by DPAS to remove assets from inventory and provide a control document of transfer of ownership. Copies of DD Form 1348s will be attached to the asset and maintained in DPAS to be cross-referenced with assets dispositioned.

(6) ADP System Reports.

Used by IT-APO to cross-reference all process points. IT-APO analyzes reports to identify discrepancies between systems and administrative control.

## 8.8. EQUIPMENT LICENSES.

To fulfill the requirements for Property Accountability, DCMA APOs will use DPAS to maintain all licenses for equipment:

a. Calculate and transmit accounting transactions to the Financial Accounting Systems (DAI).

b. Integrate with the DAI system to provide:

(1) New Receipts to be received from DAI.

(2) Asset Transfers from DoD Organizations.

(3) Asset Transfers to Contractors as GFP.

(4) Asset Transfers from Contractors to return GFP.

c. Manage Software Licenses and where the assets are installed.

d. Integrate with the IUID Registry to update all Life Cycle events for assets.

e. RFID tagging and reading capabilities to include the ability to use Real-Time Location System to locate and map assets.

f. Use of Hand-Held Devices to perform Inventories, asset relocation and UII Associations.

## 8.9. SUPPORTING DOCUMENTATION.

a. Create ADP Equipment Project (capital or non-capital) in DAI/Oracle instructions.

b. Detailed asset lists and summary schedules (reporting amounts/quantities by class of assets).

c. Contract documentation, including (for base assets and asset modifications):

(1) SOW.

(2) Contract clauses that define who owns assets and when the reporting entity takes possession; Purchase Orders.

(3) Receiving report or other acceptance document (e.g., DD Form 250).

d. Obligating documents supporting asset acquisition and any related asset improvements, such as contracts/SOWs, work orders, reimbursable agreements, MIPR, purchase orders, receiving reports and invoices, and appraisal reports for donated assets, must demonstrate how a modification increases functionality and the estimated useful life of the asset.

e. Documentation supporting any retirements, transfers, sales, or other disposal of idle, excess, obsolete, or otherwise unusable assets such as:

(1) Request for Transfer of Excess Real and Related Personal Property (GSA Form 1334, Request for Transfer of Excess Real and Related Personal Property).

(2) Declaration of Excess document.

(3) Approval documentation; documents supporting disposal start date.

(4) Documents supporting the determination of impairment from the performance of physical asset/inventory counts.

(5) DD Form 1150, "Request for Issue/Transfer/Turn-In."

(6) Documentation supporting the "placed-in-service" date (e.g., DD Form-1354, DD Form 250), including documentation supporting the useful life estimate for recognition of depreciation/amortization expense.

# SECTION 9: SMARTPHONE AND WIRELESS MOBILE DEVICE PROCESSES

**SMARTPHONE AND WIRELESS MOBILE DEVICE PROCESSES.**

a. Agency smartphones and mobile wireless devices are issued to employees for the purpose of conducting official Agency business IAW Section 2635.704 of Title 5, Code of Federal Regulations. Smartphones and all features and capabilities will be used IAW this policy. This includes voice, text, email, data, both still image and video recording capabilities; including any capability provided by installed mobile apps. Agency smartphones may be issued to employees whose responsibilities include frequent work communication while on travel and/or away from their permanent workstation, or where landline telephone service is not available.

b. Employees are allowed limited, *De Minimis* personal use of government-issued smartphones and mobile wireless devices. This personal use must not:

(1) Result in the loss of work productivity.

(2) Interfere with official duties.

(3) Result in additional expense to the government.

(4) Violate the DCMA Ethical Standards of Employee Conduct.

c. Smartphones are issued to employees, based upon their Position Based Description IT equipment Category.

d. Request to changes in an employee Position Based Deployment IT category must be initiated by their supervisor.

(1) The request for a change to the IT equipment category must be coordinated and routed through the Regional Command staff.

(2) Smartphone and mobile wireless device issuance may be denied based on Agency funds availability, determined lack of need or an employee's prior misuse of Agency resources.

e. Smartphones and mobile wireless devices are official government property.

f. Accessories include, but are not limited to, cases, and screen protectors that have been chosen and will be issued to protect the smartphone and or mobile wireless devices from damage.

g. Employees are responsible for proper safeguarding of their assigned smartphone and or mobile wireless device.

h. DCMA-owned property is to be protected to reduce the risk of loss, damage, or

destruction. Damage to agency issued smartphones will refer to and follow the process outlined in DCMA-MAN 4101-04. See Related DCMA policy on this manual's resource page.

i. Examples of damage include but are not limited to; cracked screen, and other damage as a result of not using screen protectors or protective cases.

j. CMO Commander / Executive Directors are responsible to ensure that any instance of loss, theft, and damage of DCMA-owned property are handled IAW the DoD FMR and that financial liability for loss, damage or destruction is determined.

k. The use of Agency smartphones to place calls while driving is generally prohibited and discouraged IAW the Distracted Driving Safety Act of 2004. However, DCMA issued smartphones are equipped with a built-in hands-free device that must be used for mobile voice calls in critical and time sensitive situations. Examples of critical and time sensitive situations include but are not limited a situation requiring an immediate response. The use of Agency smartphones to text message, check email, or browse the internet while driving is prohibited.

l. DCMA employees with smartphones are not authorized to make any changes to their Agency smartphone service or account. The Agency Contracting Officer or COR with the Procurement Center or DCMAIT are the only authorized agents to make any changes to the Agency smartphone accounts or services with the smartphone service provider.

m. Unauthorized or inappropriate use of Agency smartphones may result in:

(1) Loss of use of smartphone.

(2) Disciplinary or adverse action.

(3) Being held personally liable for any costs associated with the inappropriate use or damage.

n. Employees separating from the Agency must return their smartphone to DCMAIT. Failure of a separating employee to return an assigned smartphone device may result in a deduction from the employee's final paycheck.

# GLOSSARY

## G.1. ACRONYMS AND ABBREVIATIONS.

| TERM | MEANING |
|---|---|
| A2R | Acquire to Retire |
| AD | Active Directory |
| ADP | Automated Data Processing |
| APO | Accountable Property Officer |
| APS | Accountable Property System |
| APSR | Accountable Property System of Record |
| CAGE | Commercial and Government Entity |
| CIO | Chief Information Officer |
| CIP | construction-in-progress |
| CJCSI | Chairman of the Joint Chiefs of Staff Instruction |
| CMD | Commercial Mobile Device |
| CMDB | Configuration Management Database |
| COR | Contracting Officer's Representative |
| COTS | Commercial Off-the-Shelf |
| CPL | Component Property Lead |
| CST | Customer Service Technician |
| DAI | Defense Agencies Initiative |
| DAPO | Information Technology Directorate Accountable Property Officer |
| DCMA-INST | DCMA Instruction |
| DCMA-MAN | DCMA Manual |
| DCMAIT | DCMA Information Technology |
| DD | Department of Defense (used on forms only) |
| DD Form 200 | Financial Liability Investigation of Property Loss |
| DD Form 250 | Material Inspection and Receiving Report |
| DD Form 362 | Statement of Charges/Cash Collection Voucher |
| DD Form 1149 | Requisition and Invoice/Shipping Document |
| DD Form 1150 | Request for Issue/Transfer/Turn-In (Hand receipt) |
| DD Form 1348-1A | Issue Release/Receipt Document |
| DD Form 2875 | System Authorization Access Request (SAAR) |
| DFARS | Defense Federal Acquisition Regulation Supplement |
| DFAS | Defense Finance and Accounting Service |
| DISA | Defense Information Systems Agency |
| DITCO | Defense Information Technology Contracting Organization |
| DLADS | Defense Logistics Agency Disposition Services |
| DoDD | DoD Directive |
| DoD ESI | Department of Defense Enterprise Software Initiative |
| DoDI | DoD Instruction |
| DPAS | Defense Property Accountability System |

| | |
|---|---|
| ELA | Enterprise License Agreement |
| FAO | Finance and Accounting Officer |
| FAR | Federal Acquisition Regulation |
| FLIPL | Financial Liability Investigation of Property Loss |
| GFO | General or Flag Officer |
| GFP | Government Furnished Property |
| GOTS | Government off-the-shelf software |
| HRH | Hand Receipt Holder |
| IA | Information Assurance |
| IAW | in accordance with |
| IC/CIO | Office of the Chief Information Officer IT Information Technology |
| ID | Identification |
| IO | Information Owner |
| IP | Internet Protocol |
| IT | Information Technology |
| ITAM | Information Technology Asset Management |
| IT-AM | Information Technology Asset Manager |
| IT-APO | Information Technology Accountable Property Officer |
| ISO/IEC | International Standardization Organization/International Electrotechnical Commission |
| IUID | Item Unique Identification |
| IUS | internal use software |
| LAL | Local Area Network Administrator Locator |
| LAN | Local Area Network |
| LAN ADMIN | Local Area Network Administrator |
| LCM | Lifecycle Management |
| MFD | multi-functional device |
| MIPR | Military Interdepartmental Purchase Request |
| MOA | Memorandum of Agreement |
| NTV | Non-Tactical Vehicle |
| OPR | Office of Primary Responsibility |
| PA | Property Administrator |
| PC | Property Custodian |
| PED | Portable Electronic Device |
| PM | Program Manager |

| | |
|---|---|
| PP&E | Property, Plant and Equipment |
| PR | Purchase Request Form (AQP-1) |
| PWCS | Personal Wireless Communications Systems |
| PWS | performance work statement |
| RFID | radio frequency identification |
| SAM | Software Asset Management |
| SCIF | Sensitive Compartmental Information Facility |
| SES | Senior Executive Service |
| SOW | statement of work |
| SPI | Software Process Improvement |
| UIC | Unit Identification Code |
| UII | Unique Item Identifier |
| WAWF | Wide Area Workflow |

## G.2. DEFINITIONS.

| TERM | DEFINITION |
|---|---|
| **Accreditation** | Official certification that a model, simulation, or federation of models and simulations and the associated data are acceptable for use for a specific purpose. |
| **APO** | 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 their 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. |
| **Administration and general service systems** | IT systems installed on unclassified networks. |
| **Amortization/depreciation** | Asset recognition requires the proper accounting treatment (expense or capitalization with amortization/depreciation) and the reporting of capitalized amounts and accumulated depreciation/amortization on the appropriate DoD component's financial statements. For each module or component of a software project, amortization/depreciation should begin when that module or component has been successfully tested. If the use of a module is dependent on completion of another module(s), the amortization/depreciation of that module will begin when both that module and the other module(s) have successfully completed testing. |
| **Asset** | Assets are tangible or intangible items owned by the Federal Government which would have probable economic benefits that can be obtained or controlled by a Federal Government entity. A DoD asset is any item of economic value owned by a DoD component or held in a fiduciary capacity under the control of a DoD component. |
| **Auto Discovery Tool** | Applications that can audit computers and services for physical and software configuration information. |
| **Build** | A functional subset or increment of a system also known as the version. |

| | |
|---|---|
| **Business Partner Network** | The equivalent to DoD Activity Address Code and are the critical data link in identifying the responsible organization to accomplish a WAWF receiving report. |
| **Cannibalization** | Authorized removal of a specific assembly, subassembly, or part from one system for installation on another end item to satisfy an existing supply requisition and to meet priority mission requirements with an obligation to replace the removed item. Cannibalizing 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. |
| **Capitalization** | An asset that is valued and reported on the balance sheet; costs are then amortized/depreciated over an extended period of time. |
| **CIP** | The amount of direct labor, direct material, and overhead incurred in the construction of general property, plant, and equipment for which the Federal agency will be accountable. Upon completion, these costs will be transferred to the proper capital asset account as the acquisition cost of the item. This account does not close at year-end. |
| **Command, Control, Communications, and Computer Systems** | Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control, across the range of military operations. Also called "communications and information systems." |
| **CMD** | A subset of PED as defined in DoD Directive (DoDD) 8100.02 that provide one or more commercial wireless interfaces along with a compact user input interface (Touch Screen, Miniature Keyboard, etc.) and exclude PEDs running a multi-user operating system (Windows OS, Mac OS, etc.). This definition includes, but is not limited to smart phones, tablets, and e-readers. |
| **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 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. 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. |
| **COTS Software** | Software developed, tested, and sold by commercial companies to the general public. This software meets operational requirements without modification or alteration to perform on a DoD network or computer. Examples include word processors, databases, application generation, compiler, graphics, communications, and training software. |
| **CMDB** | A CMDB is a database that contains all relevant information about the components of the information system used in an organization's IT services and the relationships between those components. Typically includes hardware, software, and topology information. |
| **CST** | CSTs support customers with resolving issues relating to IT devices, such as personal computers, personal digital assistants, and printers. |
| **Designated Approving Authority** | The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority. |
| **Documentation** | Records required to plan, develop, operate, maintain, and use electronic records and software. Included are systems specifications, file specifications, code books, record layouts, user guides, and output specifications. |
| **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. |
| **Embedded software** | Computer software that is integrated into (embedded) and necessary to operate equipment. |
| **Enterprise License** | Allows the purchasing organization to use multiple copies of a specific COTS software program, usually up to a specified number, across the organization for a set price as |

| | |
|---|---|
| | a more cost-effective acquisition strategy than purchase of individual copies. |
| **Equipment Control Officer** | An individual appointed by each IT Division to manage and **(DAPO)** control IT assets resources for a site/CMO who acts as a subordinate to the applicable APO and performs inventory, utilization, and maintenance recording and reporting and other custodial duties as the APO requires. |
| **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 regarding 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. |
| **Interoperability** | The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. The condition achieved among communications-electronics systems or items of communications-electronics equipment when exchanging information or services directly and satisfactorily between them and/or their users. |
| **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. IT includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services) and related resources. Notwithstanding the above, IT does not include any equipment that is acquired by a Federal contractor incidental to a Federal |

| | |
|---|---|
| | contract. (DoDD 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009). |
| **ITAM** | IT asset management is the set of business practices that join financial, contractual and inventory functions to support life cycle management and strategic decision making for the IT environment. Assets include all elements of software and hardware that are found in the business environment. |
| **IUS in development costs** | The full cost amount incurred during the software development. |
| **License Agreements** | Contracts between the software publisher and the user that instructs and limits the software use. When purchasing software, the buyer only acquires a license to use it. The publisher retains the full rights to the software and has the sole right to its further distribution and reproduction. |
| **LCM** | (1) The management of a system or item, starting with the planning process and continuing through successive management processes and associated life-cycle management phases and associated milestones, until a system is terminated. (2) A management process, applied throughout the life of an automated information system that bases all programmatic decisions on the anticipated mission-related and economic benefits derived over the life of the automated information system. |
| **Maintenance** | (1) All action taken to retain materiel in or to restore it to a specified condition. It includes: inspection, testing, servicing, classification as to serviceability, repair, rebuilding, and reclamation. (2) All supply and repair action taken to keep a force in condition to carry out its mission. (3) The routine recurring work required to keep a facility (plant, building, structure, ground facility, utility system, or other real property) in such condition that it is continuously used, at its original or designed capacity and efficiency, for its intended purpose. (4) The function of keeping Command, Control, Communications, and Computer 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. Maintenance includes both preventive and corrective actions. Software maintenance includes anticipating, detecting, and eliminating errors. |

| | |
|---|---|
| **Models and simulations** | The use of models, including emulators, prototypes, simulators, and stimulators, whether statically or over time, to develop data as a basis for making managerial or technical decisions. A physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. |
| **Network** | Two or more computers connected to each other through a multi-user system or by other electronic means to exchange information or share computer hardware or software. |
| **Peripheral** | Any equipment that provides the IT system with additional capabilities distinct from the central processing unit (e.g., a printer, mouse, disk drive, digitizer, etc.). |
| **Program lead software** | Responsible for execution and management of the program-level software acquisition policies and procedures. |
| **Requirement** | A need for a new or improved information processing capability that, when satisfied, increases the probability of operational mission success, or decreases the cost of mission support. |
| **Resources** | Any IT system, component hardware and software, contractual services, personnel, supplies, and funds. |
| **Reuse** | The process of developing or supporting a software-intensive system using existing software assets. |
| **Simulations** | Models that are executed over time, typically on a computer, to predict system behavior. |
| **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. Any software product including commercial software, open-source software, non-commercial software, firmware used for prototyping, supporting, or executing DCMA test or mission capability. |
| **Software in development** | The activities that result in software products, including requirements analysis, design, implementation, and integration and test. |

| | |
|---|---|
| **Software enhancement** | Modifications or improvements made to a software product that provide additional functions, correct defects in earlier versions, or improve the performance, capacity, or capabilities of the software. |
| **System** | A set of IT components and their external peripherals and software interconnected with another set. The organization of hardware, software, material, facilities, personnel, data, and services needed to perform a designated function with specified results, such as the gathering of specified data, its processing, and delivery to users. Typical systems include notebook computers, desktop personal computers, networked and distributed systems (e.g., servers, workstations, data management processors, etc.), mainframe and midsize computers and associated peripherals. |
| **TEM** | Tivoli Enterprise Management System |
| **US Standard General Ledger** | A uniform chart of accounts and technical guidance for standardizing Federal agency accounting. |
| **User** | The individual who operates the computer or uses application software. |

# REFERENCES

Code of Federal Regulations, Title 32, Part 117
Committee on National Security Systems, "Security Categorization and Control Selection for National security Systems," March 27, 2014
DCMA User Access Agreement, revised February 1, 2021
DCMA Manual 3301-08, "Information Security," January 20, 2019
DCMA Manual 4101-04, "Accountable Property and General Equipment," March 3, 2019
DCMA Manual 4101-05, "Enterprise Non-Tactical Vehicles," February 23, 2019, as amended
DCMA Manual 4401-20, "Position Based Distribution of Information Technology Assets," February 26, 2024
DFARS, Subpart 217.70, "Exchange of Personal Property," August 17, 2023
DoD 7000.14-R, Volume 1, "Department of Defense Financial Management Regulations (FMRs): General Financial Management Information, Systems and Requirements," current edition
DoD 7000.14-R, Volume 4, "Department of Defense Financial Management Regulations (FMRs): Accounting Policy," current edition
DoD 7000.14-R, Volume 10, "Department of Defense Financial Management Regulations (FMRs): Contract Payment Policy," current edition
DoD 7000.14-R, Volume 12, "Department of Defense Financial Management Regulations (FMRs): Special Accounts, Funds and Programs, current edition
DoD FMR 7000.14-R, Department of Defense Financial Management Regulations (FMRs)," current edition
DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," January 10, 2013, as amended
DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," March 17, 2016, as amended
DoD Instruction 4140.73, "Asset Physical Accountability Policy," June 4, 2021
DoD Instruction 5000.64, "Accountability and Management of DoD Equipment and Other Accountable Property," April 27, 2017, as amended
DoD Instruction 5000.76, "Accountability and Management of Internal Use Software (IUS)," March 2, 2017, as amended
DoD Instruction 5000.87, "Operation of the Software Acquisition Pathway, "October 2, 2020
DoD Instruction 5330.03, "Single Manager of DoD Document Services," May 7, 2021
DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020
DoD Instruction 8320.03, "Unique (UID) Identification Standards for Supporting the DoD Information Enterprise," November 4, 2015, as amended
DoD Instruction 8320.04, "Item Unique Identification (IUID) Standards for Tangible Personal Property," September 3, 2015, as amended
DoD Instruction 8330.01, "Interoperability of Information Technology, Including National Security Systems", September 27, 2022
DoD Instruction 8440.01," DoD Information Technology (IT) Service Management (ITSM)," December 24, 2015
DoD Manual 4140.01, Volume 12, "DoD Supply Chain Materiel Management Procedures: Enterprise Logistics Decisions," May 9, 2023

DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended
DoD Manual 5205.07, Volume 1, "DoD Special Access Program (SAP) Security Manual: General Procedures." June 8, 2015, as amended
Intelligence Community Directive 503, "Intelligence Community Information Technology Systems Security Risk Management," July 21, 2015
ISO/IEC 19770-1:2017, "Information Technology IT Asset Management Systems," December 2017
ISO/IEC 20000 -1:2018, "Information Technology - Service Management," September 2018, confirmed 2023
NIST SP 800-88 Rev. 1, "Guidelines for Media Sanitization," December 17, 2014
NSA/CSS POLICY 6-22, **"**Handling of NSA/CSS Information Storage Media," 21 November 2019
NSA/CSS Policy Manual 6-22, "Handling of NSA/CSS Information Storage Media," 21 November 2019
NSA/CSS Policy Manual 9-12, "NSA/CSS Storage Device Sanitization and Destruction Manual," 4 December 2020
Office of Management and Budget Bulletin No. 16-12, "Category Management Policy: Improving the Acquisition and Management of Common Information Technology: Software Licensing," June 2, 2016
Office of Management and Budget Bulletin No. 23-13, "'No TikTok on Government Devices' Implementation Guidance," February 27, 2023
Public Law 115-91, Section 1634, "National Defense Authorization Act for Fiscal Year 2018," December 12, 2017
Public Law 115-232, Section 889, "National Defense Authorization Act for Fiscal Year 2019," August 13, 2019
Public Law 117-328, "Consolidated Appropriations Act, 2023,", Section 102, December 29, 2022
T.O. 00-33A-1001, "General Communications Activities Management Procedures and Practice Requirements," November 1, 2021
United States Code, Title 10, Section 2222