



DEPARTMENT OF THE ARMY
CHIEF INFORMATION OFFICER
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

PR-GOV-AR-033

26 June 2024

SAIS-PRP (25-1rrrr)

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Asset Accountability and Management of Internal Use Software

1. References.

a. CIO/G-6 Armywide Implementation Guidance for Accountability and Auditability of Internal Use Software, 9 April 2019 (hereby rescinded).

b. AR 25-1 (Army Information Technology).

2. Purpose: Provide additional guidance and procedures that relate to the lifecycle accountability and management of Army-owned Internal Use Software (IUS) assets.

3. Background.

a. On 9 April 2019, the CIO/G-6 issued reference 1a for Armywide implementation of guidance to account for the Army's IUS.

b. The reference 1a IUS guidance was succeeded with IUS accountability requirements in AR 25-1. The Army CIO has since determined the reference 1a guidance and the IUS content in AR 25-1 must be updated with a more efficient and effective solution to account for IUS. The enclosed manual provides detailed policy, guidance, and procedures for maintaining property management and accountability of IUS. It also defines roles and responsibilities of Army IUS property managers and other officials.

3. Guidance. Effective immediately:

a. The reference 1a document is rescinded.

b. All Army organizations must abide by and implement the roles and responsibilities, policy, guidance, and instructions in the enclosed manual for IUS accountability and management.

4. Compliance. The Army CIO may coordinate follow up audits with the Army Audit agency to assess compliance with this guidance.

SAIS-PRP (25-1rrrr)

SUBJECT: Asset Accountability and Management of Internal Use Software

5. Expiration. This guidance remains in effect until superseded or rescinded.

6. Review. The OCIO Policy Division (SAIS-PRP) will review this guidance annually no later than 1 October of each calendar year.

7. Points of contact:

a. CIO Policy Inbox: usarmy.pentagon.hqda-cio.mbx.policy-inbox@army.mil.

b. IUS lead for OCIO: Ms. Michelle West at michelle.p.west3.civ@army.mil.

GARCIGA.LE
ONEL.T.1186
170411

Digitally signed by
GARCIGA.LEONEL.T.11
86170411
Date: 2024.06.26
16:22:11 -04'00'

Encl

LEONEL T. GARCIGA
Chief Information Officer

DISTRIBUTION:

Principal Officials of Headquarters, Department of the Army
Commander

U.S. Army Forces Command
U.S. Army Training and Doctrine Command
U.S. Army Materiel Command
U.S. Army Futures Command
U.S. Army Pacific
U.S. Army Europe and Africa
U.S. Army Central
U.S. Army North
U.S. Army South
U.S. Army Special Operations Command
Military Surface Deployment and Distribution Command
U.S. Army Space and Missile Defense Command/Army Strategic Command
U.S. Army Cyber Command
U.S. Army Medical Command
U.S. Army Intelligence and Security Command
U.S. Army Corps of Engineers
U.S. Army Military District of Washington
U.S. Army Test and Evaluation Command
U.S. Army Human Resources Command
U.S. Army Corrections Command
U.S. Army Recruiting Command

Superintendent, U.S. Military Academy

Commandant, U.S. Army War College

(CONT)

SAIS-PRP (25-1rrrr)

SUBJECT: Asset Accountability and Management of Internal Use Software

DISTRIBUTION: (CONT)

Director, U.S. Army Civilian Human Resources Agency

Executive Director, Military Postal Service Agency

Director, U.S. Army Criminal Investigation Division

Director, Civilian Protection Center of Excellence

Director, U.S. Army Joint Counter-Small Unmanned Aircraft Systems Office

Superintendent, Arlington National Cemetery

Director, U.S. Army Acquisition Support Center

CF:

Principal Cyber Advisor

Director of Enterprise Management

Director, Office of Analytics Integration

Commander, Eighth Army



U.S. Army Office of the Chief Information Officer

ASSET ACCOUNTABILITY AND MANAGEMENT OF INTERNAL USE SOFTWARE



June 2024

Enclosure



CONTENTS

1. INTRODUCTION	1
PURPOSE	1
2. GENERAL INFORMATION	1
2.1 APPLICABILITY.....	1
2.2 POLICY	2
3. RESPONSIBILITIES	4
3.1 ARMY CIO.....	4
3.2 DEPUTY CHIEF OF STAFF, G-6 (DCS, G-6)	5
3.3 ASSISTANT SECRETARY OF THE ARMY (FINANCIAL MANAGEMENT & COMPTROLLER) (ASA (FM&C))	5
3.4 ASSISTANT SECRETARY OF THE ARMY (ACQUISITION, LOGISTICS AND TECHNOLOGY (ASA (ALT))	5
3.5 SYSTEM OWNER	6
3.6 REPORTING RESPONSIBILITIES FOR MANAGING IUS ASSETS	6
4. PROCEDURES.....	7
4.1 IUS ASSET IDENTIFICATION	7
4.2 IUS ASSET ACCOUNTABILITY	7
4.3 CAPITALIZATION PROCEDURES	9
4.4 APSR PROCESSES.....	9
4.5 DATA ELEMENTS.....	10
4.6 VALUATION.....	12
REFERENCES.....	13



1. INTRODUCTION

PURPOSE

In accordance with issuance from the Deputy Secretary of Defense (reference 1), this manual—

- Provides additional guidance and procedures for Army implementation of the requirements of Section 11316 of the Clinger-Cohen Act (reference 2), and the direction of the Under Secretary of Defense (Comptroller), Deputy Chief Financial Officer (reference 3) that relate to the lifecycle accountability and management of Internal Use Software (IUS), to include documenting IUS lifecycle events and transactions.
- Provides guidance on IUS criteria consistent with Department of Defense (DoD) Financial Management Regulation (FMR) 7000-14-R (reference 4), and Army Regulation (AR) 25-1, Army Information Technology (reference 5).
- Establishes policies, assigns responsibilities, and provides procedures for maintaining property management and accountability of Army-owned IUS.
- Defines the roles and responsibilities of Army IUS property managers and other officials regarding IUS property management and accountability.
- Identifies Army Accountable Property System of Record (APSR) procedures.

2. GENERAL INFORMATION

2.1 APPLICABILITY

This issuance applies Armywide to—

2.1.1. Headquarters, Department of the Army, Army Commands, Army Service Component Commands, and all other Direct Reporting Units (referred to collectively in this manual as the “Army”).

2.1.2. Property management, accountability requirements and financial reporting for IUS as defined by this policy. Personal accountability for security-related matters is addressed by DoD Instruction (DoDI) 8500.01 (reference 6). This issuance does not issue policy for financial accounting or audit of IUS. Financial accounting requirements for IUS are addressed by DoD 7000.14-R. Audit readiness requirements are addressed through the Financial Improvement and Audit Readiness (FIAR) Guidance (reference 7).

ASSET ACCOUNTABILITY AND MANAGEMENT OF INTERNAL USE SOFTWARE



2.1.3. IUS that is acquired through appropriated or working capital funds including those transferred to the Army for implementation but not developed by the Army.

2.2 POLICY

The Army—

2.2.1 Defines IUS as having both of the following characteristics: (1) the software is acquired, internally developed, or modified solely to meet the entity's internal needs; and (2) during the software's initial development or modification (post deployment development), no substantive plan exists or is being developed to market the software externally.

2.2.2. Manages all software including IUS to ensure resources are used efficiently and effectively, in accordance with Subtitle III of the Clinger-Cohen Act.

2.2.3. Maintains accountability over IUS as defined in this policy until formally relieved of accountability when IUS is removed from use per DoD 7000.14-R.

2.2.4. Performs fiduciary reporting of expenses and capitalization of IUS defined in this policy in accordance with DoD 7000.14-R and the Statement of Federal Financial Accounting Standards Number 10 for the DoD (reference 8).

2.2.5. Maintains property management and accountability of IUS system records, financial cost evaluation, authoritative asset tracking as authoritative data in Army business systems and transactional ledgers with auditable accounting using APSRs.

2.2.6. Applies the following criteria to software for determination of what software shall be defined as IUS consistent with law and DoD Policy:

- Embedded Software in Weapons Systems (see reference 9: AR 71-9, Warfighting Capabilities Determination): IUS does not include software that is integrated into and necessary to operate military equipment. For the Army, this includes all software required for an operational force to execute a warfighting function that is not linked to a Defense Business System. Criteria for this category include software acquired in support of an Army Requirements Oversight Council approved requirement as defined in AR 71-9 and is operated by a deployable unit or a unit apportioned to Combatant Commands. Frequently, but not always, such software operates on equipment identified with a Line Item Number (LIN) on military unit Mission Table of Organization and Equipment (MTOE).
- Offensive and Defensive Cyber Operations: IUS does not include software developed for the Cyber Mission Force mission. Offensive and Defensive cyber

ASSET ACCOUNTABILITY AND MANAGEMENT OF INTERNAL USE SOFTWARE



operation tool development has been approved by the Army Requirements Oversight Council and are directed by U.S. Cyber Command. These tools represent Military Equipment for the Cyber Mission Force and their supporting organizations and so are exempt.

- Defense Business Systems (DBS) (see reference 10: AR 5-1, Management of Army Business Operations): All Defense Business System (DBS) as defined by AR 5-1 are covered IUS. The methods for how the DBS are acquired will determine if financial reporting and asset accountability are required, such as, an accounting determination will be required to enumerate which DBS costs should be capitalized or expensed.
- Network Common Services (AR 25-1): All software utilized to provide network common services to provide the Army Information Technology Service Catalogue services are not IUS. They are embedded software for the operation of the network. Such software includes Software Defines Wide Area Network software controllers, cloud common services, and communication capabilities.
- Perishable Software: IUS does not include software acquired or internally developed that is perishable in nature as measured by no validated Army requirements processes in accordance with AR 5-1, AR 25-1, or AR 71-9. For the Army, this includes all software developed as part of episodic training, tools created for demonstration purposes only, or Science and Technology research that do not produce software for operational use.
- Low code/No code Activity within an Approved Software Platform: IUS does not include Low-code/No Code activity within a software platform approved by the Army Chief Information Officer (CIO) for this purpose. As long as the activity does not expand the scope of the approved platform, the activity is utilization of software for its intended purpose as in not new.
- Infrastructure as Code: Infrastructure as code is the ability to provision and support a computing infrastructure using code instead of manual processes and settings. Examples of low code/no code activity include utilization of macros within common office products, open source data transformations within a data platform, employing machine language automation within the core capabilities of the environment, or scripts within an Artificial Intelligence training suite. Infrastructure as Code: IUS does not include low-code/code activities (e.g., scripts) for direct management of the network, operating systems, and system infrastructure. These are inherently embedded software for the system the activity controls.
- Army Working Capital Fund (AWCF): Capital IUS that is funded by the AWCF will be reported on the AWCF Financial statements. This will be purchased as part of

ASSET ACCOUNTABILITY AND MANAGEMENT OF INTERNAL USE SOFTWARE



the Capital Investment Program. All other capital IUS will be reported on the General Fund statements.

2.2.7. Applies the following criteria for IUS reporting purposes, in particular those IUS requiring the reporting of expenses and capitalization as defined in DoD 7000.14-R and the Statement of Federal Financial Accounting Standards Number 10:

- As-a-service acquisition: Software acquired through commercial offerings of Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) are by their nature not owned by the government and are only licensed. If the license is annually renewed, they are expensed items and so do not require capitalization financial reporting.
- Annual licenses: Software acquired through annual licensing is by its nature expensed as the software is not a government asset with enduring value.
- Annual maintenance fees: Annual software maintenance fees are by their nature an expensed activity. Conducting life cycle maintenance on a software based capital asset where the activity does not require development funding is also by its nature an expensed activity as it does not add value to the software asset. However, if the underlying software being maintained was purchased with ownership rights by the government, the software may require capitalized financial reporting per 2.2.5–6 above and in accordance with DoD 7000.14-R.

3. RESPONSIBILITIES

3.1 ARMY CIO

The Army CIO—

3.1.1. Establishes Army policy and guidance for all information technology (IT) including definition, management, accountability, and audit of IUS assets.

3.1.2. Develops, approves maintains and oversees Army IUS policy in accordance with the Clinger-Cohen Act and AR 25-1.

3.1.3. Oversees Army IT resource management (ITRM), IT Portfolio Management (ITPM), IT reporting and IT accountability through the Army Portfolio Management Solution (APMS) and the Defense IT Portfolio Reporting (DITPR) system via the Department of Defense Chief Information Officer (DoD CIO).



3.2 DEPUTY CHIEF OF STAFF, G-6 (DCS, G-6)

The DCS, G-6 implements policies and strategies related to Army unified network operations, cybersecurity and ITRM, to include assisting IUS fiscal documentation in Army Planning, Programming, Budgeting and Execution (PPBE) systems.

3.3 ASSISTANT SECRETARY OF THE ARMY (FINANCIAL MANAGEMENT & COMPTROLLER) (ASA (FM&C))

The ASA (FM&C)—

3.3.1. Provides accounting and financial management policy and guidance for IUS, including, but not limited to, valuing, depreciating, and reporting of IUS in accordance with the requirements outlined in DoD 7000.14-R, Vol. 4, Ch. 27.

3.3.2. Establishes resource management, execution and cost accounting guidance on software acquisition, development, and implementation.

3.3.3. Establishes policy, guidance and functional data management oversight for Army financial systems and designation of the APSR for IUS.

3.3.4. Ensures accounting level detail and data elements identified in this policy to achieve consistency between business processes including the Deputy Assistant Secretary of the Army (Cost and Economics) (DASA (CE)) developed cost positions, program evaluations, alignment through contracts at the CLIN/SLIN level, use of standard Army accounting codes and development of the Army IUS financial statement.

3.4 ASSISTANT SECRETARY OF THE ARMY (ACQUISITION, LOGISTICS AND TECHNOLOGY) (ASA (ALT))

The ASA (ALT)—

3.4.1. Is the HQDA authority for oversight and policy for all Army acquisition. Executes and manages the Army-wide Procurement Management Review Program.

3.4.2. Serves as senior Army enterprise level staff for providing management, oversight, and evaluation of Army software procurement, contracting and acquisition activities.

3.4.3. Ensures compliance of procurement and contracting responsibilities assigned by statute and regulation (references 11–16).



3.5 SYSTEM OWNER

The system owner—

3.5.1. Is responsible for ensuring IT investments and IUS are accounted for in APMS. All IUS cover by this policy that require cationization must be registered in APMS and have a unique Army IT Resource (AITR) number assigned.

3.5.2. Ensures contracts written for the acquisition, development, and life cycle maintenance of IUS are written to the level of specificity that allows for clear classification and work breakdown structure (WBS). Validates alignment to financial execution and reporting requirements for both a capital expensed and expensed activities for IUS asset.

3.5.3. Ensures development of IUS-related Contract Line-Item Numbers (CLINs) and Sub Line-Item Numbers (SLINs) structure. Provides guidance for both requesting activities and contracting officers to clearly segregate capital from non-capital costs.

3.5.4. Identifies the Program Manager and/or Resource Manager and the Authorizing Official for the system and ensures that system scope and boundaries are consistent across financial, property, and cybersecurity management systems.

3.6 REPORTING RESPONSIBILITIES FOR MANAGING IUS ASSETS

System owners identify the Program Manager (PM) and/or Resource Manager (RM) to perform these reporting responsibilities—

3.6.1. Review program documentation to ensure proper accounting classification and accounting treatment, to include WBS or Performance Work Statement (PWS), Cost Breakdown Structure (CBS) or Independent Government Cost Estimate (IGCE).

3.6.2. Review and structure software requirement deliverables to separate activities for software development from other activities, in accordance with DoD FMR 7000-14R, Volume 4, Chapter 27 guidance.

3.6.3. Register the capitalization date of IUS in APMS as a mandatory part of “go/no go” decision criteria for deployment and updated annually.

3.6.4. Obtain the dated record of technical acceptance test, placed in service date, contractor deliverables, and invoices, and provide these to the appropriate Army or DoD APSR.

3.6.5. Supporting documentation must be retained to address financial reporting responsibility and right to recognize and record. This will meet financial reporting

ASSET ACCOUNTABILITY AND MANAGEMENT OF INTERNAL USE SOFTWARE



requirements when Army transfers in an IUS asset from another component of Department of Defense (DOD) or Agency.

3.6.6. IUS asset inventory capitalization procedures are outlined in documentation that defines methodology used, how verified capital IUS asset is still in use, and which documentation demonstrates existence. Perform IUS asset inventory procedures and provide evidence upon request.

3.6.7. Maintain property management and accountability of Capital IUS records and performs fiduciary reporting of capitalized IUS, using approved accountable property system of record (APSR).

3.6.8. The system accountable records are validated to ensure the associated auditable information is available for examination. This may include substantiating documentation, validating the completeness of records, and proving the IUS exists. Guidance for required IUS data elements is found in Section 4.5 Data Elements.

4. PROCEDURES

4.1 IUS ASSET IDENTIFICATION

4.1.1. Internally developed software refers to software that employees of the entity are actively developing, including new software, and existing or purchased software that are being modified with or without a contractor's assistance.

4.1.2. Contractor-developed software refers to software that a federal entity is paying a contractor to design, program, install, and implement, including new software and the modification of existing or purchased software.

4.1.3. Software associated with Department of Defense Information Network–Army (DoDIN-A) operations are part of U.S. Cyber Command Mission (USCYBERCOM) set and so are not considered IUS.

4.1.4. System owners will use the criteria identified within Section 2.2.6–7 of this document for IUS determination and as required an assignment of a system PM or RM for proper IUS accountability.

4.2 IUS ASSET ACCOUNTABILITY

4.2.1. All IUS will be registered in APMS and will be assigned a unique AITR number. The Army will establish accountable records in an APSR for all capitalized IUS, expensed software, and expensed software lifecycle management activities.

ASSET ACCOUNTABILITY AND MANAGEMENT OF INTERNAL USE SOFTWARE



4.2.2. IUS that meets the definitions in this policy and has an initial capitalization threshold of \$250,000 and have a useful life of two years or more in accordance with FMR 7000.14-R. IUS meeting these criteria will be recorded as a capitalized asset in an APSR.

4.2.3. A single record will be created in APMS for each IUS purchase or acquisition and all costs incorporated in accordance with the DoD 7000.14-R guidance.

4.2.4. A single record for must be created for each distinct manufacturer part number on each purchase order for a bulk license purchase for COTS software. The quantity field on the IUS record will represent the total sum of all licenses with the corresponding manufacturer part number on the record. License information associated with the quantity of licenses will be included in the record for the purchase or acquisition, as applicable.

4.2.5. The Army will maintain accountable records for non-capital IUS expenses in an APSR or managerial system.

4.2.6. The Army will maintain accountable records for the life of the asset and will retain the records in accordance with National Archives and Records Administration's (NARA's) standards, as described in NARA Directive 1571 and supplemented by Chapter 9, Volume 1 of DoD 7000.14-R.

4.2.7. Accountable records will contain the data elements defined in Paragraph 4.5. The IUS property records will provide a system transaction history suitable to support an audit and act as the authoritative source for validating the existence and completeness of the IUS inventory.

4.2.8. The system PM/RM is responsible for maintaining supporting documentation or evidentiary material suitable for audit. The PM/RM will maintain such documentation (hard copy or electronic copy of original documentation) in a readily available location, during the applicable retention period. This will permit the validation of information pertaining to the IUS, such as purchase cost, purchase date, license entitlements, evidence of delivery of developed IUS, and cost of improvements.

4.2.9. Supporting documentation may include, but is not limited to, purchase invoices, procurement contracts, receiving documents, technical documents, and licensing agreements. Acceptable supporting documentation information is prescribed in the FIAR Guidance.

4.2.10. The Army will maintain records and supporting documentation in accordance with DoDI 5015.02 and Chapter 9, Volume 1 of DoD 7000.14-R.

4.2.11. At any point in time, the Army will report an IUS property record in a single APSR for fiduciary purposes. Fiduciary reporting consists of capitalized IUS information

ASSET ACCOUNTABILITY AND MANAGEMENT OF INTERNAL USE SOFTWARE



to be used in the Army accounting systems. IUS property records may exist in multiple systems for management purposes, to include configuration management or license management.

4.2.12. The Army will maintain accountable records for IUS provided by the Army on contracts funded through the general fund and the AWCF. These records will document software changes, requirements, and architectures.

4.3 CAPITALIZATION PROCEDURES

Instructions for the capitalization process—

4.3.1. Follow the guidance in DoD 7000.14-R, Vol. 4, Ch. 27.

4.3.2. Use Army standard accounting codes and ledger accounting procedures as defined for IUS by ASA (FM&C).

4.3.3. Follow FMR on development versus modification consistent with fiscal law definitions for use of research, development, test, and evaluation (RDTE) and operations and maintenance (O&M) determination.

4.3.4. The PM/RM will utilize the criteria in Section 2.2.6–7 to assist with identification of expensed items given Army software policy.

4.3.5. For RDTE appropriated in Budget Activity 8 (BA8) the Army will use fiscal law definitions as they apply to the software lifecycle to account for capital costs and what should be expensed.

4.4 APSR PROCESSES

A single Army implemented APSR for IUS will—

4.4.1. Act as a sub-ledger to the accounting system of record for the Army in accordance with Chapter 6, Vol. 4 of DoD 7000.14-R.

4.4.2. Be updated by the Army, as required, to keep information timely.

4.4.3. Contain (at minimum) the data required for an accountable property record, in accordance with Section 4.5.

4.4.4. Perform accountability functionality, as required of an APSR.



4.4.5. Synchronize data with DoD CIO repository systems (e.g., SNaP-IT, DoD Information Technology Portfolio Repository (DITPR)), as directed by the Army CIO.

4.4.6. Hold the complete inventory of capitalized IUS assets purchased or developed by the Army in APMS.

4.4.7. Hold non-capitalized IUS unless a managerial system(s) with sufficient controls in place is implemented. The Army Primary APO may approve, in writing, such a managerial system only if it meets the requirements of this issuance when used for non-capitalized IUS accountability and includes appropriate managerial controls.

4.5 DATA ELEMENTS

As per DODI 7500.76, the Army's APSR will maintain the following data elements, at a minimum, for IUS accountable property records. The elements are divided into "general" and "capital" categories for applicability purposes. Both "general" and "capital" elements are required for capital IUS property accountability in the Army's APSR. Only the "general" data elements are required for non-capital IUS property accountability in either an APSR or approved managerial system. The responsibility for the accuracy of the data in APMS and GFEBS, respectively, resides with the full end-to-end business process and internal control environment. An overview of the source system and functional responsibility for each required IUS data element can be found in Figure 1: IUS Source System.

4.5.1. General Data Elements:

- (1) DoD Unique Software Identifier.
- (2) Item name or software title.
- (3) Item description.
- (4) Software type (COTS, modified COTS, modified government off-the-shelf, custom).
- (5) Original manufacturer part number or original manufacturer Stock Keeping Unit number (if applicable).
- (6) Software developer (publisher).
- (7) Version (if applicable).
- (8) Quantity of licenses (if applicable).
- (9) Hosting environment (i.e., cloud-based, client/server, local).
- (10) National stock number or catalog equivalent (if applicable).
- (11) Location (e.g., of the hosting server, network, COTS license agreement, purchase order terms and conditions, installation media).
- (12) Status (e.g., active, pending disposal, transferred).
- (13) IT budget UII.
- (14) PSC (if applicable).

ASSET ACCOUNTABILITY AND MANAGEMENT OF INTERNAL USE SOFTWARE



4.5.2. Capital Data Elements:

- (1) Requiring (i.e., reporting) DoD Component's DoDAAC.
- (2) Parent system (e.g., Enterprise Resource Planning system) by DoD Unique Software Identifier number (as applicable).
- (3) System Sub-system (e.g., Enterprise Resource Planning module) DoD Unique Software Identifier (as applicable).
- (4) Placed in service date (i.e., acceptance date, FDD).
- (5) General Ledger Classification.
- (6) General Ledger Accounting Code.
- (7) Gross asset value (i.e., full cost, acquisition cost).
- (8) Useful life.
- (9) Accumulated amortization.
- (10) Obligating document number or posting reference.
- (11) Accountable or responsible party.
- (12) Standard Line of Accounting.
- (13) Transaction type.
- (14) Transaction data

IUS Data Element	Source System	Functional Owner
DoD Unique Software Identifier	APMS	APMS Owner
Item Name or Software Title	APMS	APMS Owner
Item Description	APMS	APMS Owner
Software Type	APMS	APMS Owner
Original Manufacturer Part Number/Stock Keeping Unit Number	APMS	APMS Owner
Software Developer	APMS	APMS Owner
Software Version	APMS	APMS Owner
Quantity of Licenses	APMS	APMS Owner
Hosting Environment	APMS	APMS Owner
National Stock Number or Catalog Equivalent	APMS	APMS Owner
Location	APMS	APMS Owner
Status	APMS	APMS Owner
IT Budget UII	APMS	APMS Owner
PSC	APMS	APMS Owner
Requiring DoD Component's DoDAAC	GFEBs	ASA(FM&C)
System Sub-System DoD Unique Software Identifier	GFEBs	ASA(FM&C)
Placed in Service Date	GFEBs	ASA(FM&C)
General Ledger Classification	GFEBs	ASA(FM&C)
General Ledger Accounting Code	GFEBs	ASA(FM&C)
Gross Asset Value	GFEBs	ASA(FM&C)
Useful Life	GFEBs	ASA(FM&C)
Accumulated Amortization	GFEBs	ASA(FM&C)
Obligating Document Number or Posting Reference	GFEBs	ASA(FM&C)
Accountable or Responsible Party	GFEBs	ASA(FM&C)
Standard Line of Accounting	GFEBs	ASA(FM&C)
Transaction Type	GFEBs	ASA(FM&C)
Transaction Data	GFEBs	ASA(FM&C)

Figure 1: (U) IUS Data Element Source System



4.6 VALUATION

IUS will be capitalized at full cost, which is comprised of the acquisition cost and other applicable costs. When acquisition cost is unknown, reasonable estimates of the historical acquisition cost may be used. See DoD 7000.14-R for IUS valuation procedures.



REFERENCES

1. Deputy Secretary of Defense memorandum (Establishment of the Office of the Under Secretary of Defense for Research and Engineering and the Office of the Under Secretary of Defense for Acquisition and Sustainment), July 13, 2018.
2. The Clinger-Cohen Act, 40 U.S.C., Subtitle III, Section 11316 (1996).
3. Under Secretary of Defense (Comptroller), Deputy Chief Financial Officer memorandum (Accounting Policy Update for Financial Statement Reporting for Real Property Assets), September 30, 2015.
4. DoD 7000.14-R, (Financial Management Regulation), date varies by volume.
5. AR 25-1 (Army Information Technology).
6. DoDI 8500.01 (Cybersecurity).
7. Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer issuance (Financial Improvement and Audit Readiness (FIAR) Guidance), April 2016.
8. Federal Accounting Standards Advisory Board (Statement of Federal Financial Accounting Standards Number 10: Accounting for Internal Use Software: Technical Release 5), May 14, 2001.
9. AR 71-9 (Warfighting Capabilities Determination).
10. AR 5-1 (Management of Army Business Operations).
11. Federal Acquisition Regulation (FAR).
12. DoD FAR Supplement (DFARS).
13. Army FAR Supplement (AFARS).
14. AR 70-13 (Management and Oversight of Service Acquisitions),
15. AR 715-30 (Secure Environment Contracting)
16. AR 715-31 (Army Competition Advocacy Program)
17. NARA Directive 1571 (National Archives and Record Administration—Part 1234: Electronic Records Management), February 21, 2006.

ASSET ACCOUNTABILITY AND MANAGEMENT OF INTERNAL USE SOFTWARE



18. DoDI 5015.02 (DoD Records Management Program), February 24, 2015, as amended.
19. DoDD 5144.02 (DoD Chief Information Officer (DoD CIO)), November 21, 2014, as amended.
20. DoDD 8000.01 (Management of Department of Defense Information Enterprise (DoD IE)), March 17, 2016, as amended.
21. DoDI 5000.02 (Operation of the Defense Acquisition System), January 7, 2015, as amended.
22. DoDI 5000.64 (Accountability and Management of DoD Equipment and Other Accountable Property), May 19, 2011, as amended.
23. DoDI 5230.24 (Distribution Statements on Technical Documents), August 23, 2012, as amended.
24. DoDI 8320.03 (Unique Identification (UID) Standards for Supporting DoD Net-Centric Operations), November 4, 2015, as amended.
25. DoDM 8910.01 (DoD Information Collections Manual: Procedures for DoD Internal Information Collections), Vol. 1, June 30, 2014, as amended.
26. DoDM 4160.21 (Defense Material Disposition), October 22, 2015, as amended.
27. ASTM International E-2131 (Standard Practice for Addressing and Reporting Loss, Damage, or Destruction of Tangible Property), current edition¹.
28. ASTM International E-2132-11 (Standard Practice for Inventory Verification: Electronic and Physical Inventory of Assets), current edition¹.