ACQUISITION AND MANAGEMENT OF VA INFORMATION TECHNOLOGY RESOURCES

1. **REASON FOR ISSUE:** This Directive revises Directive 6008 issued in November 2017 and establishes policy for the acquisition and management of information technology (IT), IT-related and other assets and resources, across the Department of Veterans Affairs (VA). VA's IT, IT-related and other assets and resources are core resources of the Department and their effective management is critical to the provision of services to our Nation's Veterans. This directive only pertains to the type of funding that can be used for procuring resources. This oversight is necessary to ensure alignment of items throughout VA enterprise to the information management information assurance policies, VA wide rules, standards and guidance. Additionally, this policy ensures that all IT funded and IT-related assets are acquired within the constraints and intent of the VA's IT Systems appropriations account, providing specific guidance as to when IT-related assets must be funded through IT Systems account or other authorized accounts. In consultation with VA Administrations and offices, all of VA's IT and IT-related assets and resources and services are subject to the laws, executive mandates and policies of the VA Chief Information Officer (CIO). This includes information assurance, security and privacy; enterprise architecture, standards and specifications; and IT management, technical and operational internal controls, regardless of the funding source, unless otherwise indicated by appropriation, regulation, or policy. This policy, which replaces all previous memoranda on this subject, is necessitated by the growing magnitude and speed of change in information technologies, network-attached devices (i.e., the "Internet of Things (IoT)") and information security risks, procedures and regulations. Its full implementation will improve VA’s effectiveness in the use of resources to deliver a standardized, integrated, interoperable and Veteran-centric information environment in accordance with all Federal laws, regulations and industry best practices.

2. **SUMMARY OF CONTENTS/MAJOR CHANGES**: This directive supersedes VA Directive 6008 dated November 2, 2017. This directive reaffirms the VA CIO's oversight authority over all IT- related assets regardless of funding source and requesting office as highlighted by the Federal Information Technology Acquisition Reform Act (FITARA).

    a. Clarifies the CIOs authority and role in planning, programming, budgeting and execution (PPBE) of all IT resources; clarifies the definition for IT, IT-related and other assets and resources; and expands language on funding sources.

    b. Specifies that any VA IT and/or IT-related asset and resource, or service, that stores, transmits, manipulates, displays, or supports VA information assets, shall comply with all laws, executive mandates and VA CIO policies regarding IT.

c. Provides policy, guidance and principles on the use of the VA IT Systems appropriations account and other VA appropriations for the acquisition, development and operation of VA IT and IT related assets in a secure, consistent, effective and efficient manner, as directed by congressional authority.

d. Establishes rules and standards relative to enterprise-wide management of IT and IT-related resources are published as part of VA's Enterprise Architecture and governed by the IT Investment Board.

3. **RESPONSIBLE OFFICE:** Assistant Secretary for Information and Technology (005), Information Technology Resource Management (ITRM) (005F).

4. **RELATED HANDBOOK**: None.

5. **RESCISSION**: VA Directive 6008, Acquisition and Management of VA Information Technology Resources dated November 2, 2017.

CERTIFIED BY:

/s/
Guy T. Kiyokawa
Assistant Secretary for
Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Kurt DelBene
Assistant Secretary for
Office of Information and Technology
and Chief Information Officer.

Distribution: Electronic Only

TABLE OF CONTENTS

ACQUISITION AND MANAGEMENT OF VA INFORMATION TECHNOLOGY ASSETS

1. **PURPOSE AND SCOPE:** This directive establishes policy for the funding of development, acquisition, operations and management of Information Technology (IT), IT-related and other assets and resources across the Department of Veterans Affairs (VA). See Appendix B Explanatory Notes # 1 through 3 for clarification of IT, IT-related and other assets and resources. As the accountable official for the management and security of all of VA's IT resources, including but not limited to, VA's operational information and associated resources such as personnel, equipment and funds, VA's Chief Information Officer (CIO) has authority over all IT and IT- related assets that are part of, or interact with, VA's information networks, systems, services and capabilities. This policy:

   a. Clarifies the scope of VA's IT, IT-related and other assets and resources.

   b. Specifies that any VA asset, resource, or service, that stores, transmits, manipulates, or displays VA information shall comply with all IT and IT-related laws, executive mandates and policies.

      (1) All IT, IT-related and other assets and resources must comply with all laws, executive mandates and policies regarding information assurance, security and privacy; enterprise architecture, standards and specifications; IT management, technical and operational controls, regardless of the funding source and requesting office.

      (2) IT, IT-related and other assets and resources must conform to all VA policies governing connection to the VA network.

   c. Affirms all VA IT, IT related and other assets and resources connecting to the VA Network, regardless of funding source and requesting or managing office, are subject to those rules, standards and oversight processes as prescribed by the VA CIO and VA policy. This directive clarifies and strengthens the ability of the VA CIO to manage enterprise compliance with value measurement, architecture, accessibility and information assurance standards, in accordance with Congressional direction/mandate and the highest standards of public transparency and resource stewardship.

   d. Ensures all IT and IT-related assets within VA are developed, procured and operated in the most effective and efficient manner possible within the legal limitations of VA appropriations and other relevant information resource management laws and regulations.

   e. Defines those circumstances under which assets must be developed, acquired, or operated with the IT Systems appropriations account (or other funding source authorized to acquire IT and IT-related assets) and those circumstances under which they may be acquired by VA organizations and facilities with other funds. If any asset connects to the VA Network, IT policies governing security and maintenance must be followed.

f. Assigns roles and responsibilities related to the funding and management of VA's IT, IT- related and other assets and resources.

g. Specifies that acquisition of all IT and IT-related assets shall be strictly limited to acquisition vehicles that adhere to VA IT policies such as cybersecurity and accommodation for persons with disabilities.

h. Reinforces VA's use of life cycle management and total cost of ownership in the planning and management of all IT, IT-related and other assets and resources planned for or deployed in VA.

i. States that VA items/services not purchased from the IT Systems account or other authorized accounts are to be funded by the appropriate Administration or Staff Office with the allowable appropriations account or fund.

2. POLICY.

a. A Federal Information Technology Acquisition Reform Act (FITARA) Review is required for all requirements with IT and IT-related capabilities (including cloud services) utilizing OMB's Information Technology and Telecommunications Product Service Codes (PSCs), regardless of funding appropriation, funding source and dollar value as outlined in accordance with policy. These assets and resources must adhere to the policies and processes of IT and IT-related assets. The review is conducted in the Budget Tracking Tool (BTT) under the Acquisition Review Module (ARM) which expands the CIO's accessibility and visibility on IT procurements in accordance with FITARA. For additional information contact the Office of Strategic Sourcing at: Ask Strategic Sourcing

b. Funded with IT Systems Account and other Authorized Accounts.

(1) Generally, only the IT Systems appropriations account, the Franchise Fund, Supply Fund, Veterans Canteen Fund, the Office of the Inspector General (OIG) account, the VA/Department of Defense (DoD) Joint Incentive Fund, Electronic Health Record Modernization (EHRM) account and VA/DoD Federal Health Care Center Joint Fund have the legal authority to fund VA IT items (hardware, software and services), subject to the laws and regulations governing these Funds. IT items are identified as those utilizing the Office of Management and Budget's (OMB) Information Technology and Telecommunications Product Service Codes (PSC).

(2) IT products for delivery to Veterans provided by benefits programs under Title 38 authorities will not be charged to the IT Systems account but have explicit legal authority to reimburse the IT Systems account.

(3) VA IT funded items and services include but are not limited to:

(a) All IT networks and equipment except networks and equipment on either the Medical Device Isolation Architecture (MDIA) or Specialized Device Isolation Architecture (SDIA).

(b) All commercially developed software for the VA, except for Commercially available off-the-shelf (COTS) software used exclusively for items funded without IT funds as specifically defined in this directive (except for those systems funded by accounts other than IT as noted in section 2.c. of this directive).

(c) VA developed software application costs, including the development, acquisition, product support and management of the software applications, as well as any associated open source, innovations or pilots.

(d) Any interface, mechanism, or service for providing access to applications in any IT environment operating under VA control, including private/commercial cloud operations, except items funded from accounts other than those that fund IT (i.e., Software as a Service (SaaS)).

(e) IT systems administration training, IT development and testing environments, IT performance testing, IT life cycle planning and IT technical requirements gathering (but not including business requirements gathering).

(f) VA IT infrastructure (i.e., servers, storage, networks) required to maintain IT funded persistent data sources, both authoritative and non-authoritative and legacy stores, including all data storage (on premises and cloud based), backup and disaster recovery capabilities (except those items listed in section 2.c. of this directive).

(g) Voice, data and video telecommunications infrastructure (i.e., circuits and switches, wired cabling to the wall), regardless of whether the space is owned or leased by VA.

(h) Patch cabling requiring IT funding includes:

i IT funded device to wall jack;

ii Patch panel to distribution switch in the telecom closet; and

iii Patch panel in server room to core routers in server room.

(i) Telecommunications and telephone services and equipment except dedicated lines or services to patient residences for telemedicine.

(j) All enterprise and limited number software and software licenses (except for those systems funded by accounts other than IT as noted in section 2.c).

(k) Employee and contractor support for IT help desk and customer service operations.

(l) Other service models used in VA's IT production environment, such as infrastructure-as-a-service (IAAS), platform-as-a-service (PAAS) and telecommunications-as-a-service, as defined by the National Institute of Standards and Technology's (NIST) guidelines, that require VA maintenance and/or interfaces to VA's IT production environment, applications, or data stores.

(m) All mixed-use systems, computers and mixed-use servers, (i.e., those that support both OIT offices and other VA administration offices).

(n) Single focal point for VA cloud policy and VA Enterprise Cloud (VAEC) environment.

(o) Assessment, planning, management and migration for VA Enterprise Cloud infrastructure.

(p) IT support for Veterans Canteen Service (VCS) that is provided to other components of VA, such as use of VA network servers and installation and maintenance of security software. However, VCS is responsible for funding all costs (including related sustainment) that are specific only to VCS or VCS operations, such as Point of Sale (POS) systems.

c. Accounts other than those that fund IT, IT-related and Other Assets and Resources referenced in Section 2.b. of this directive:

(1) VA IT related assets are to be funded by the requesting Administrations or Staff Offices, including related subsequent operations and maintenance costs, using its proper appropriation. VA's offices and administrations requiring IT resources (i.e., interfaces, network storage) for IT, IT-related and other asset requirements must have a plan to fund their entire set of requirements prior to completing a procurement. If an IT-related or other asset procurement has IT dependencies, it is the responsibility of the requesting office to comply with OIT intake processes to ensure available IT resourcing and funding for all requirements prior to the start of the project (i.e., hosting, operations and maintenance support). The funding must be programmed in compliance with the funding requirements of this directive.

(2) Medical and Clinical Systems, Equipment, Devices, or Software (MCSEDS) which meets one or more of the following criteria or definitions.

NOTE: The definitions of the terms mentioned in Section 2.c.(2) can be found in section 5: Definitions of this directive:

(a) Medical Device.

(b) Medical Device as defined by Food and Drug Administration (FDA).

(c) Medical Device Data System (MDDS) as defined by FDA; see Definitions section 5.

(d) Clinical System.

(e) Clinical Information System (CIS).

(f) Clinical Decision Support (CDS) tool.

(g) A mobile medical application (app) which meets the FDA definition of a Medical Device.

(h) This includes the procurement, development and ongoing maintenance and operations costs of the mobile medical app. This includes the costs of hosting and services related to the management of medical apps in the VA Enterprise Cloud but does not include the app store itself, which is an IT “persistent data source” and as such requires IT management and funding.

(i) Computers, tablets, mobile devices and accompanying data services (data plans) that are supplied to a clinician running MCSEDS applications and/or meets one or more of the MCSEDS criteria or definitions. Any non-medical applications on a device (i.e., e-mail) must be funded by IT.

(j) Telehealth equipment, which includes devices to report symptoms and measure vital signs for Veterans in their homes and the equipment necessary to connect Veterans and clinicians virtually via interactive video sessions, as well as the technology used to collect, store and forward telehealth information for clinical treatment purposes.

(k) Medical systems, equipment, or devices required in support of medical training and simulation.

(l) Computers and servers which are non-severable components of a medical device system (i.e., diagnostic imaging, Picture Archiving and Communication System (PACS), Clinical Information Systems (CIS), etc.).

(m) Any MCSEDS that has an FDA product code.

(n) Any MCSEDS that do not otherwise meet the definitions above and/or are not regulated by the FDA but aid in the:

i Diagnosis, treatment, or monitoring of a patient, including but not limited to telehealth, radiology, cardiology, pulmonary, anesthesia, laboratory, intensive care unit and surgery systems and/or;

ii Investigation, replacement, modification, or support of the anatomy or of a physiological process and which does not achieve its principal intended action in or on the human body by pharmacological, immunological, or metabolic means, but which may be assisted in its function by such means and/or;

iii Single and/or dedicated medical function, either directly or in support of another medical device, clinical service or application that directly impact a patient's health care, (i.e., Biological Refrigeration (Blood Banks), etc.), Optical Fabrication, Pharmacy packaging equipment, Nurse Call systems, Radio- Frequency Identification/real-time location system and Temperature Monitoring systems.

(3) Commercially available Off-The-Shelf (COTS) Software for Direct Patient Care items are purchased solely for purposes of direct patient care, as defined herein and/or meets one of more of the definitions listed under section 2.c. of this directive.

(4) Office Equipment and Office Supplies.

(a) High-capacity multifunction devices that have copying, emailing and/or printing capabilities within one device and support a large office or workgroup.

(b) Office supplies, including consumables and peripherals for end-users. This includes anything that attaches to a computing device that does not store or process information, but rather serves just as an input or output device. Examples include privacy screens, bar code readers, monitors, headsets, insurance card readers, microphones, speakers, wireless keyboards, mice and mouse pads and desktop Uninterruptible Power Supply (UPS) units.

(c) 3D printers, models, software and services used to manufacture physical objects are considered additive manufacturing devices.

(5) Facility Equipment includes industrial control equipment, fire alarms, building automation systems, building security systems, digital signage systems, energy efficient lighting monitors/transmitters, information boards/electronic signage, elevator systems, carrier neutral distributed

antenna systems, carrier neutral cell repeater sets/boosters and Uninterruptable Power Supplies (UPS) except small desktop UPS.

(6) Construction Projects includes modifications to a building's infrastructure even though required specifically for IT purposes, the acquisition and installation of a wire closet fiber optic infrastructure, power surge protection, distribution and battery backup systems and heating, ventilation and air conditioning (HVAC) equipment to comply with either operating requirements and/or manufacturer warranties. This includes construction of data centers. However, the IT Systems account, Franchise Fund, Supply Fund, Veterans Canteen Fund, EHRM account and OIG account do ***not*** have the legal authority to incur any construction or cabling costs associated with major or minor construction, Non-Recurring Maintenance (NRM) projects and station level construction projects.

(7) Cabling infrastructure:

(a) Device funded by accounts other than IT to wall jack.

(b) All patch panel to patch panel and patch panel to wall jack cabling (including but not limited to behind the wall, above the ceiling or under the floor).

(c) Servers in a server room connecting to core routers (Including but not limited to security systems or biomedical devices).

(8) Purchase or migration of applications to VA OIT Managed Cloud Environments funded from accounts other than those that fund IT:

(a) Any IT purchase that requires IT funding, if not operated on the cloud, remain an IT funding requirement if migrated to, or purchased for, usage in the cloud.

(b) Similarly, any IT related purchase that is allowable for funding from accounts other than those that fund IT, if not operated on the cloud, remain allowable for funding from accounts other than IT if migrated to, or purchased for, usage in the cloud.

(9) Miscellaneous VA IT-related Products and Services.

(a) Information Technology Assets Purchased by a Vendor:

i IT related hardware procured by a vendor incidental to a Federal contract and required to support the performance of that contract, will be funded by the same appropriations account(s) as the contract if the hardware is not used by any VA employee or connected to any VA network, except through an approved Virtual Private Network (VPN) such as the Citrix Access Gateway (CAG).

ii Any IT asset, as defined by this policy, procured by a vendor incidental to a contract and intended to be turned over to the VA must comply with all VA asset management and security policies and be procured using an IT funding source.

(b) Software-as-a-Service (SaaS) solutions where the software is not owned or hosted by VA and no additional capabilities were added as a customization of the software and made part of the procurement. Also, the user must log on to a vendor site where all the functionality is made available and the vendor must be responsible for software, hardware, data security, help desk, etc. functions. See Appendix C, of this directive, for the SaaS approval process.

(c) Costs of IT-related items and services funded by non-VA grants or other non-VA funding sources, such as non-VA research efforts.

(d) IT-related assets for delivery to Veterans provided by benefits programs under Title 38 authorities.

(e) Business process re-engineering. (This does not include associated software and infrastructure costs).

(f) End-user training costs, including train-the-trainer costs are the responsibility of the benefitting organization(s) to pay for their users as the system is deployed.

(g) Networks, wired or wireless, provided for patient care and therapeutic use for the benefit of Veterans and/or their family that are not connected to any VA network.

(h) Web content creation (such as textual copy, photos, video), services and management. (NOTE: This only pertains to content creation and does not pertain to software development of websites).

(i) Compensated Work Therapy purchases exclusively supported by reimbursements from clients to support the program.

(j) Specific bequests or gifts of funds to the VA for the purchase of IT products or services will be deposited in the General Post Fund and funded from the General Post Fund. This is a legally authorized augmentation of the IT Systems account.

d. Other Internal Controls.

(1) The Chief Financial Officer (CFO) or other designated official for each VA Administrations and Staff Office must submit an annual certification letter to the Office of Information & Technology CFO. This letter shall state that to

the best of their knowledge no funding outside of the IT Systems account will be used to procure IT assets, as defined by this policy.

(2) Administration and Staff Office CFOs, other designated officials and/or program managers shall immediately coordinate with the OIT CFO should they become aware of any non-conformity to this policy.

(3) The VA IT Workgroup (ITW) shall review and interpret IT related acquisitions' questions, as they relate to VA Directive 6008 and appropriations law, to make decisions about whether a specific project requires IT Systems account funding or is allowable for funding from accounts other than those that fund IT, when this policy does not allow for a clear determination. Issues that cannot be resolved by the ITW will be forwarded to the VA CFO Council for resolution.

3. RESPONSIBILITIES.

a. **Assistant Secretary for Information and Technology**, as the Department's CIO, in planning, managing and overseeing the VA's information resources shall:

(1) Plan, program, budget and execute the IT Systems appropriations account.

(2) Define the IT Strategic Plan and objectives of the organization, aligning this Plan to the larger VA strategic objectives and ultimately providing review, concurrence, or requisite feedback on IT acquisition strategies/plans, regardless of funding source.

(3) Ensure VA optimizes standardization, interoperability, security, reliability and flexibility of the technology infrastructure across the enterprise, as well as adherence to information protection standards and initiatives. Monitors alignment of IT programs and systems for consistency with the Department's Strategic Plan, Administrations and Staff Offices Lines of Business priorities, IT Strategic Plan and Enterprise Architecture.

(4) Manage approved reimbursable budget transfers when required to move the applicable funding between affected organizations.

(5) Design, develop, implements and maintain a VA IT governance structure to:

(a) Ensure the proper use of the IT Systems appropriations account and acquisition of VA enterprise IT capabilities.

(b) Ensure that this policy is maintained and revised as required based on changing technologies**.**

(c) Ensure that the ITW SharePoint Portal and intake process is maintained and updated as new decisions or documentation become available Link: https://dvagov.sharepoint.com/sites/VHAITRMITFMOS/SiteAssets/ITNONITV2/IT NonIT.aspx

(d) Implement the policies to set criteria for whether a given asset or service is funded by the IT Systems account or not.

(e) Ensure all VA information resources, including those funded outside the IT Systems appropriations account, are compliant with enterprise policy, rules, standards and guidance related to IT, information management (IM) and information security (IS) and FITARA.

(f) Provide visibility through the VA's enterprise architecture to all policies, rules, standards, guidance and configurations necessary to guide VA IT and IT-related item design, acquisition, development and deployment.

(g) Develop, maintain and assure completeness and proper use of standard IT configurations.

(h) Establish, maintain and make available bulk buy and enterprise purchase programs for IT and IT-related assets (including assets such as end user devices which may be purchased outside the IT Systems appropriations account) and services to ensure standardization, interoperability, economies of scale and accessibility of VA information environment.

(i) Oversee and collaborates with VA stakeholders at the local level to ensure that IT and IT-related capabilities, funded and deployed at local sites, are appropriately vetted and aligned to enterprise policies, rules, standards and guidance, including FITARA. Ensure that the operations and sustainment costs for all IT and IT-related acquisitions at the local level are properly funded.

(j) Integrate compliance with this policy within decision processes that OIT oversees or participates in.

b. **Under Secretaries, Assistant Secretaries and Other Key Officials** shall:

(1) Ensure all VA IT and IT-related items/services which connect to any VA Network follow rules, standards and oversight processes as prescribed by the VA CIO in order to comply with information assurance, accessibility, security, privacy and enterprise architecture standards.

(2) Integrate compliance with this policy within established decision processes in which they oversee or participate.

(3) Maximize collaboration with the open source OIT community; and

(4) Plan, program and budget for VA IT-related items/services to ensure they are supportive of VA Administration and Staff Office requirements.

(5) Ensure all VA IT and IT-related items/services that meet the OMB definition of IT comply with all Federal laws and regulations and VA enterprise policies, rules, standards and guidance related to IT, information management (IM) and information security (IS) and FITARA.

c. **The Office of General Counsel** provides appropriate legal advice and interpretation of appropriations law, as necessary, to assist in determining whether a given appropriations account or Fund proposed to be used to acquire IT or IT-related resources has legal authority to fund the proposed acquisition. This advice and interpretation will also aid in determining whether an item must be purchased with the IT Systems appropriations account or not.

4. REFERENCES.

a. 21 CFR Parts 862-892-FDA Medical Device Classification Panels

b. 48 CFR § 2.101(b) Definitions Electronic Code of Federal Regulations (eCFR)

c. 29 USC § 794d: Disabled VA Employees and Members of the Public

d. 38 USC §§ 5705, 5701 and 7332: Protection of Medical Records

e. 40 USC § 11101, Definitions and SUBTITLE III: Information Technology Management and The Clinger-Cohen Act of 1996

f. 44 USC chapter 35: Information Resources Management

g. 44 USC § 3501-3521: Paperwork Reduction Act of 1995 (PRA)

h. 44 USC § 3541-49, Dec 2014: Federal Information Security Modernization Act of 2014 (FISMA)

i. Consolidated Appropriations Act, 2002, S-515, Information Quality Act (also known as the Data Quality Act)

j. Federal Information Technology Acquisition Reform Act: Title VIII, Subtitle D of the National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291

k. OMB Circular No. A-11: Preparation, Submission and Execution of the Budget

l. OMB Circular No. A-130, Management of Federal Information Resources

m. OMB Memorandum (M-06-16) Protection of Sensitive Agency Information (June 23, 2006)

n. OMB Memorandum M-12-18, Managing Government Records Directive, Aug 2012

o. OMB Memorandum M-15-14, June 10, 2015: Management and Oversight of Federal Information Technology

p. OMB Memorandum (M-19-13) Category Management: Making Smarter Use of Common Contract Solutions and Practices

q. Public Law 107-347, December 2002: E-Government Act of 2002

r. Public Law 117-103, Division J, March 15, 2022: Military Construction, Veterans Affairs and Related Agencies Appropriations Act, 2022

s. Public Law 111-352, Jan 2011: Government Performance Results Act (GPRA) of 2010

t. VA Directive 6300, Records and Information Management

u. VA Directive 6500, VA Cybersecurity Program (formally Managing Information Security Risk: VA Information Security Program)

v. VA Directive 6517, Risk Management Framework for Cloud Computing Services.

w. VA Directive 6518, Enterprise Information Management

x. VA Directive 6550, Pre-Procurement Assessment for Medical Device/Systems

y. VA IT Workgroup (ITW) Technical Working Group Charter (formally VA IT/Non-IT Workgroup Charter)

z. VA OGC Memorandum opinion, “Information Technology (IT) Support to the Veterans Canteen Service” (Mar. 2019)

aa. VAOPGCADV 6-2015, “Use of the Franchise Fund to Purchase Information Technology Services and Systems (Apr. 2015)

5. DEFINITIONS:

a. **Acquisition Review Module (ARM).** ARM is the tool of record that expands the accessibility and visibility in accordance with the Federal Information Technology Acquisition Reform Act (FITARA). ARM combines the acquisition, budget and technical reviews that streamlines the acquisition approval process and provides the ability to track and approve IT and IT-related procurement and process decisions.

b. **Application.** (See OMB Circular A-130 Appendix III) The use of information resources (information and information technology) to satisfy a specific set of user requirements.

c. **Authoritative Data Source**. A source of data or information designated and recognized as official that is trusted, timely, secure and used within VA's information environment in support of VA business processes. An authoritative data source is the one and only (logical) location where a respective data element is created, updated and deleted. Administrations and Staff Offices designate these sources within domains for which they are the stewards. The Office of Information and Technology may develop and maintain technology solutions (i.e., services) that use these sources. [VA Directive 6518, Enterprise Information Management Policy]

d. **Authority to Operate (ATO).** The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations and the Nation based on the implementation of an agreed-upon set of security controls.

e. **Clinical.** Pertaining to actual observation and treatment of patients, as distinguished from theoretical or experimental.

f. **Clinical Decision Support.** Clinical decision support (CDS) provides clinicians, staff, patients or other individuals with knowledge and person-specific information, intelligently filtered, or presented at appropriate times, to enhance health and health care. CDS encompasses a variety of tools to enhance decision-making in the clinical workflow. These tools include computerized alerts and reminders to care providers and patients; clinical guidelines; condition-specific order sets; focused patient data reports and summaries; documentation templates; diagnostic support and contextually relevant reference information, among other tools. This does not include tools that only provide administrative support for clinical staff.

g. **Clinical Information System.** A Clinical Information System (CIS) is a computer-based system that is designed for collecting, storing, manipulating and making available clinical information concerning the diagnosis/treatment of patients' healthcare. Clinical Information Systems provide a repository that stores clinical data, such as the patient's history of illness and the interactions with care providers. The repository encodes information capable of helping physicians decide about the patient's condition, treatment options and wellness activities as well as the status of decisions and actions undertake.

h. **Clinical System.** Defined as a health IT system, inclusive of server infrastructure, workstations, middleware and software which facilitate clinical functions, decisions and tasks. Typically, clinical systems collect, store, analyze, retrieve, display and/or print information related to patient care within one or more clinical specialties. This includes systems that provide Clinical Decision Support.

i. **Clinician.** The term clinician refers to a healthcare professional qualified in the clinical practice of medicine. Clinicians are those who provide: principal care for a patient where there is no planned endpoint of the relationship; expertise needed for the ongoing management of a chronic disease or condition; care during a defined period and circumstance, such as hospitalization; or care as ordered by another clinician. Clinicians may be physicians, nurses, pharmacists, or other allied health professionals (which includes, but is not limited to, pharmacy staff, laboratory staff, respiratory staff, clinical social workers, medics and paramedics).

j. **Cloud computing. (Or cloud).** Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

k. **Cloud Credits.** Process to pay for cloud computing services available from the VA Enterprise Cloud (VAEC) service providers, via the Enterprise Cloud Solutions Office (ECSO) procurement vehicles established to provide migration and sustainment services in support of the VAEC.

l. **Commercially available off-the-shelf** (**COTS**) **software** is a term for software products that are ready-made and available for purchase in the commercial market. Public sector organizations are relying more and more on COTS applications to supplement, enhance or replace proprietary systems

m. **Configuration.** The administrative set-up (look & feel, access constraints, global parameters, etc.) of the front end of an application or system to adhere to network requirements. (See also definition for Interface.)

n. **Data.** An elementary description of things, events, activities and transactions recorded, classified and stored, but that may not be organized to convey any specific meaning. Data items can be numeric, alphabetic, figures, sounds or images. A database consists of stored data items organized for expeditious use, including reading, updating and deleting.

o. **Direct Patient Care.** Care of a patient provided by a clinician or staff member. Direct patient care may involve many aspects of the health care of a patient, including monitoring, diagnosis, treatments (and execution of treatment plans, i.e., dietary restrictions, etc.), care plans, counseling, or self-care by a Veteran

where medical devices are used in support of telecare (i.e., wound cameras), patient education and the administration of medication. This includes products or services which provide clinical decision support, such as those which support clinical telecare triage done by clinicians.

p. **Enterprise IT Capabilities.** Enterprise level IT capabilities built using IT resources and data that are shared across two or more organizational components regardless of location. Within the VA this includes all IT-related services for Veterans and eligible beneficiaries, support functions and resource management. Embodied in this concept are technical efforts such as infrastructure engineering for building, managing and evolving shared IT; IT or infrastructure operations for administering and monitoring the performance of the IT service being provided to the enterprise; and IT services management. Efforts such as IT strategy, portfolio management and IT governance enable this concept to function effectively.

q. **Federal Information Technology Acquisition Reform Act (FITARA)**. A law that puts Federal agency CIOs in control of agency IT investments. FITARA was enacted in response to specific Federal IT challenges, such as duplication of IT spending between and within agencies, understanding cost & performance of Federal IT investments, providing more visibility into IT spending with an ability to benchmark IT spending within Federal entities and between Federal and private-sector counterparts.

r. **Information.** Any communication or representation of knowledge such as facts or data, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. This definition includes information that an agency disseminates from a web page.

s. **Information Environment.** The aggregate of the information created and used by an organization; the information architecture of the organization (models, authoritative and redundant data stores, data flows); the governance framework and policies and standards that ensure information is managed as an asset.

t. **Information Lifecycle.** The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage and disposition.

u. **Information Management.** The planning, budgeting, manipulating and controlling of information throughout its life cycle.

v. **Information Resources.** (See 44 USC § 3502) Information and related resources, such as personnel, equipment, funds and information technology.

w. **Information System.** (See 44 USC § 3502) A discrete set of information resources organized for the collection, processing, maintenance, transmission

and dissemination of information in accordance with defined procedures, whether automated or manual.

x. **Information Technology.** (See 40 USC § 1110 and OMB M-15-14)

(1) With respect to an executive agency, any equipment, interconnected system, or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the executive agency. This includes if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use:

(a) of that equipment; or

(b) of that equipment to a significant extent in the performance of a service or the furnishing of a product.

(2) Includes computers, ancillary equipment (including imaging peripherals, input, output and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service) and related resources; but

(3) Does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

(4) When “IT” is referenced in this document it is meant to describe all requirements/acquisitions funded with congressionally IT appropriated funds.

y. **Infrastructure.** The substructure or underlying foundation, platform or network used for providing goods and services, including communications facilities, cable, wiring, data centers, power plants and communication systems.

z. **Infrastructure as a Service (IaaS).** The capability provided to the consumer to provision processing, storage, networks and other fundamental computing resources where the consumer can deploy and run any software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, deployed applications and possibly limited control of select networking components (i.e., host firewalls).

aa. **Interface.** A shared boundary across which two or more separate components of a computer system exchange information. The exchange can be between software, computer hardware, peripheral devices, humans and combinations of these (see also configuration)

bb. **IT Asset.** Any equipment, interconnected system, or subsystem of equipment, which in whole or by virtue of component parts, are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the Executive Agency.

cc. **IT Infrastructure.** The term IT Infrastructure is applied to a group defined by OMB Circular A-11 Section 300 to include infrastructure, office automation and telecommunications. These are defined in OMB Circular A-11 Section 300 as "… all IT investments that support common user systems, communications and computing infrastructure. These investments usually involve multiple mission areas and might include general Local area Network (LAN)/Wide Area Network (WAN), desktops, data centers and cross-cutting issues such as shared IT security initiatives and telecommunications." (OMB A-11 Section 300)

dd. **IT Network.** The grouping of two or more computer systems that are physically or virtually linked together.

ee. **IT Managed Services.** A solution delivered by an IT managed service provider to supply certain IT processes and functions. Services include network, application, infrastructure and security, via ongoing and regular support and active administration. Services can be provided on customers' premises, in the service provider's data center (hosting), or in a third-party data center. Beyond traditional application and infrastructure management, managed services may also include storage, desktop and communications, mobility, help desk and technical support. (Everything that falls outside of the NIST definition of SaaS)

ff. **IT Project.** Includes projects for software development, mobile applications, hardware installations, network upgrades, cloud computing/external hosting and virtualization rollouts, enterprise architecture, information assurance, business analytics, data management projects and the implementation of IT services.

gg. **IT Related.** Products and services that may have IT components but are not required to be funded by the IT Systems appropriations account. Items are identified under OMB's Specialized Information Technology and Telecommunications Product Service Codes, Appendix B, regardless of dollar amount and includes interagency acquisitions of IT/IT-related requirements.

hh. **IT Shared Services.** The consolidation of IT operations used by multiple parts of the same organization. The goal of a shared services delivery model is to allow

each organization within the entity to focus its limited resources on activities that directly support that organization's mission. Thus, the providing organization effectively becomes an internal service provider.

ii. **Medical Device**. Any device or system that meets one or more of the following requirements:

(1) Used in patient healthcare for diagnosis, treatment (therapeutic), or physiological monitoring of patients. This includes server-based medical equipment and clinical systems. Examples of medical devices/systems include, but are not limited to, physiological monitoring systems, ventilators, infusion pumps, Computed Tomography (CT) scanners, MUSE cardiology information system, Picture Archiving and Communication Systems (PACS), Clinical Information Systems (CIS) and laboratory analyzers. This includes medical devices that directly connect to a patient; process human and other biologic specimens; create medical images, display electrophysiological waveforms; obtain physiologic measurements and/or directly perform therapeutic support to the patient.

(2) Has gone through the Food and Drug Administration's (FDA) Premarket Review or 510(k) Process.

(3) Is incorporated as part of a medical device system in such a fashion that if modified the device or system component could have a negative impact on the functionality or safety of the main medical device/system.

(4) Is determined to be a medical device by VHA Healthcare Technology Management (HTM) Program Office.

jj. **Medical Device (as defined by FDA).** An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, similar or related article, including a component part or accessory, which is:

(1) Recognized in the official National Formulary, the United States Pharmacopoeia, or any supplement to them and/or;

(2) Intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease in man or other animals and/or;

(3) Intended to affect the structure or any function of the body of man or other animals and which does not achieve any of its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes.

kk. **Medical Device Data System (MDDS) (as defined by FDA).** Medical Device Data System (MDDS) is software or hardware solely intended to

provide one or more of the following uses, without controlling or altering the functions or parameters of any connected medical devices, which may or may not be intended for active patient monitoring:

(1) The electronic transfer or exchange of medical device data.

(2) The electronic storage and retrieval of medical device data.

(3) The electronic conversion of medical device data from one format to another.

(4) The electronic display of medical device data.

(5) This may include any assemblage or arrangement of network components that includes specialized software expressly created for a purpose consistent with the intended use in the MDDS regulation.

ll. **Medical Device Isolation Architecture (MDIA).** A standard process for isolating and securing networked medical devices using a protected Virtual Local Area Network (VLAN) structure for each medical device protected by a MDIA Access Control List (ACL).

mm. **Medical mobile apps as defined by FDA**. Software programs that run on smartphones and other mobile communication devices. They can also be accessories that attach to a smartphone or other mobile communication devices, or a combination of accessories and software. Mobile medical apps are medical devices that are mobile apps, meet the definition of a medical device and are an accessory to a regulated medical device or transform a mobile platform into a regulated medical device.

nn. **Multi-Function Device Printer.** A free-standing device that has copying, emailing and/or printing capabilities within one device and supports a large office or workgroup with high-capacity functionality (i.e., # of pgs. per minute).

oo. **Other assets and resources.** All requirements/acquisitions for assets and resources that have a technology component that are not identified under Specialized Information Technology and Telecommunications Product Service Codes, Appendix B, regardless of dollar amount.

pp. **Patient**. An individual who is receiving needed professional services that are directed by a licensed practitioner of the healing arts toward the maintenance, improvement, or protection of health, or lessening of illness, disability, or pain**.** Patients receiving treatment by VA clinicians includes Veterans, family members, civilians and employees receiving health care services.

qq. **Pick and Stick.** There are situations in which either of two appropriations can be construed as available for a particular object, but neither can

reasonably be called the more specific of the two. In such instances, the "pick and stick" rule applies as follows: where two appropriations are available for the same purpose, the agency must "pick" only one account to cover expenses related to that purpose and "stick" with that account – unless it notifies Congress of its desire to change the funding mechanism through the annual budget process.

rr. **Platform as a Service (PaaS).** The capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

ss. **Redundant information.** Multiple information stores of the same information that are synchronized and/or reconciled with one another for availability, integrity and continuity purposes.

tt. **Service.** A mechanism to enable access to a set of one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description or contract.

uu. **Software as a Service (SaaS**). Software as a Service (SaaS) is an application delivery model in which the application is hosted on a cloud infrastructure outside the security boundary of VA and is provided to the Cloud Service Customer (CSC) over the internet. The CSC uses the SaaS offering via a thin-client interface, such as a web-browser or a program interface. The CSC subscribes to the SaaS offering and is only responsible for limited application configuration settings. The Cloud Service Provider (CSP) offering the application is responsible for management of the application, safeguarding of data stored or processed by the application and all elements of the underlying infrastructure. The SaaS Product shall possess limited functionality in a disconnected or offline mode.

(1) To qualify as SaaS for use at VA and to align with Federal Risk and Authorization Management Program (FedRAMP) requirements, the hosting for the offering must conform to the NIST 800-145 definition of Cloud Computing and thus contain following key characteristics:

(a) On-Demand Self-Service: The CSP fully automates the provisioning of both the customer interface and the underlying cloud components of the SaaS offering. In some cases, to the CSP may provision internal resources manually, while providing the CSC an automated interface to request and track the service.

(b) Broad Network Access: The SaaS capabilities are available over the internet or over a network that is available from all access points the CSC requires. The SaaS offering is accessible through common platforms (i.e., mobile phones, tablets, laptops and workstations).Resource Pooling: The computing infrastructure supporting the SaaS offering is shared among more than one CSC using a multi-tenant model and resources are dynamically assigned depending on customer demand.

(c) Rapid Elasticity: Computing capabilities are automatically provisioned and released in a manner that scales with customer demand. In some cases, the scaling of resources may not be fully automated, but it should be fast enough to support the needs of the CSC, which the CSC would have to define.

(d) Measured Service: Resource usage, such as storage, processing, bandwidth and user activity are measured and reported on in a manner that is relevant to the SaaS offering.

(2) The user cannot request or make any changes to the software code, except for limited user-specific application configuration settings. Any thin client/program interface shall be limited to enhancing how VA connects to the cloud service provider's infrastructure and network. The thin client/program interface shall be included in the SaaS subscription and is prohibited from being a stand-alone, on-premise offering. Any thin client/program interface is subject to VA OIT policies for downloading software. See Appendix C, of this directive, for the SaaS approval process.

vv. **Software Development.** The activity of computer programming, documenting, testing and bug fixing involved in creating and maintaining applications and software frameworks involved in a System Development Life Cycle (SDLC) and resulting in a software product. While the term refers to a process of writing and maintaining the source code, in a broader sense it includes all that is involved between the conception of the desired software through to the final manifestation of the software, ideally in a planned and structured process. Therefore, software development may include research, new development, prototyping, modification, reuse, re-engineering, maintenance or any other activities that result in Software **products.** All software development in the VA, whether Class 1, 2 or 3, shall fall under this policy guidance.

ww. **Scientific computing.** When a scientific instrument is driven by a PC/laptop or other CPU containing device, where the instrument is non-functional without that CPU/operating system and application. The computer is functionally embedded in the instrument. For example, software used to interpret electroencephalograms, audiograms, or other complex waveforms, software used to manipulate and interpret three- dimensional radiographic images (CT, MRI, etc.).

xx. **Specialized Device Isolation Architecture (SDIA)**. See Special Purpose System.

yy. **Special Purpose System**. A non-medical, network-connected system that supports building safety, security and/or environmental controls and cannot obtain a VA-approved baseline configuration due to vendor-controlled system policies, proprietary software and other system-specific controls and configurations. Special purpose systems are defined as network-connected devices that do not have the standard Visibility to Server (V2S) VA baseline configuration. Special purpose systems play a vital role in maintaining and supporting the patient experience, infrastructure, safety and/or security systems and environmental controls at VA facilities. Examples of SPS include, but are not limited to, energy management systems, heating, ventilation and air conditioning (HVAC), temperature controls, building/facility access controls and security camera systems.

zz. **System.** The same as a General Support System defined in OMB Circular A-130- Appendix III, as an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications and people. Some examples of systems are a local area network (LAN) including smart terminals that supports a branch office; an agency-wide backbone; a communications network; a departmental data processing center including its operating system and utilities; a tactical radio network or shared information processing service organization.

aaa. **System Development Life Cycle (SDLC).** Is a term used to describe a systematic approach and process for planning, creating, testing, deploying and retiring information systems.

bbb. **Telecommunications.** A universal term that is used for a vast range of information- transmitting technologies such as mobile phones, land lines, VoIP and broadcast networks. It encompasses the infrastructure of a telecommunications network and includes any lines, apparatuses, towers, antennas, or structures used, or for use in, a telecommunications network. In telecommunications, data is transmitted in the form of electrical signals known as carrier waves, which are modulated into analog or digital signals for transmitting information.

ccc. **Vendor Managed Services for the Business**. A single tenant software solution that is not owned or hosted by VA. These services are purchased for COTS applications on a subscription basis only and are hosted in a cloud environment external to the VA network and accessible via a web browser and, if available, a downloadable thin client/program interface. VA does not manage or control the underlying infrastructure including network, servers, operating systems, storage,

or even individual application capabilities except for limited user-specific application configuration settings.

ddd. **Wi-Fi.** A facility allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.

APPENDIX A: ACQUISITION AND MANAGEMENT OF VA INFORMATION TECHNOLOGY ASSETS

1. The chart below identifies the proper funding source for products and services.

2. After proper planning, budgeting and coordination with OIT the items designated as "IT Systems Account or Other Authorized Accounts/Funds" require procurement using the IT congressionally appropriated funds.

3. Products and services designated as "Accounts Other than those that fund IT" may be procured by the requesting VA Administration or Staff Office using a VA appropriation authorized for that purpose and subject to pick and stick requirements in Federal appropriations law.

4. **Definition of funding sources can be referenced under Section 2.b and 2.c.** All products and services listed require FITARA compliance.

Item Number	**Item Description**	**FUNDING SOURCE** IT Systems Account or Other Authorized Accounts/Funds	**FUNDING SOURCE** Accounts Other than those that fund IT
HARDWARE			
1	PC, laptops, tablets, smartphones, cell phones (non-Smartphones), Satellite phones. See Appendix B – Explanatory Notes 4 and 5.	X	X
2	Thin Client. See Appendix B – Explanatory Notes 4 and 5.	X	X
3	IT infrastructure (i.e., servers, storage, networks, switches and SFP Modules) required to maintain persistent data sources, both authoritative and non-authoritative and legacy stores, including all data storage, backup and disaster recovery capabilities. See Appendix B – Explanatory Notes 4 and 5.	X	X
4	Printer. See Appendix B – Explanatory Notes 4 and 5.	X	X
5	Tape Drive. See Appendix B – Explanatory Notes 4 and 5.	X	X
6	Modem. See Appendix B – Explanatory Notes 4 and 5.	X	X
7	Document Scanner.	X	
8	All Uninterruptable Power Supplies (UPS)		X

Item Number	**Item Description**	**FUNDING SOURCE** IT Systems Account or Other Authorized Accounts/Funds	**FUNDING SOURCE** Accounts Other than those that fund IT
	& Power Distribution Units (PDU) Computer Room UPS/PDU Systems and UPS equipment for individual PCs, servers, etc.		
9	Storage System (SAN, NAS). See Appendix B – Explanatory Notes 4 and 5.	X	X
10	Converged and hyper-converged virtualization solutions. See Appendix B – Explanatory Notes 4 and 5.	X	X
11	External Disk Drives. See Appendix B – Explanatory Notes 4 and 5.	X	X
12	Networking Equipment (WAN, LAN, WLAN-Wireless local Area network). See Appendix B – Explanatory Notes 4 and 5.	X	X
13	Cyber and Information Security Servers and Appliances.	X	
14	Telephone Systems (PBX, KSU, IP).	X	
15	Two-way Radios (Police, Engineers, etc.) (Facility Equipment).		X
16	Pagers (requiring telecommunications).	X	
17	Overhead Paging Systems (Facility Equipment).		X
18	Nurse Call Systems.		X
19	Handsets, Speakerphones, Conference Phones.	X	
20	Videoconferencing Endpoints. See Appendix B – Explanatory Note 6.	X	
21	Videoconferencing Bridges (Multipoint Control Unit (MCUs)).	X	
22	Peripherals (mouse, keyboard, PIV reader, bar code readers, monitors, speakers, microphones, headphones, headsets, webcams, etc.) excluding new activation and initial set-up of new employees' standard workstation, which are IT. (Office Supplies)		X
23	Supplies and Consumables (Storage media (USB drives, CD/DVD-R/RW), paper, toner, batteries). (Office Supplies)		X

Item Number	**Item Description**	**FUNDING SOURCE** IT Systems Account or Other Authorized Accounts/Funds	**FUNDING SOURCE** Accounts Other than those that fund IT
24	Digital Cameras (Clinical or otherwise), Editing Equipment.		X
25	Data Cables – cabling from IT funded device to wall jack, patch panel to distribution switch in the telecom closet and patch panel in server room to core routers in server room.	X	
26	Data Cables – cabling from devices funded from accounts other than those that fund IT to wall jack, all patch panel to patch panel and patch panel to wall jack cabling (Including but not limited to behind the wall, above the ceiling or under the floor) and from funded servers in a server room connecting to core routers (Including but not limited to security systems or biomedical devices).		X
27	Cable installation associated with a project funded from accounts other than those that fund IT (i.e., Major/Minor Construction or Non-Recurring Maintenance (NRM) - station-level projects) and cable installation that is inside the walls of a facility.		X
28	3D Printing (Hardware, software, printing materials and patterns/models).		X
29	Medical and Clinical Systems, Equipment, Devices, or Software (MCSEDS) - Bio-Medical Systems Equipment (Picture Archiving and Communication System (PACS), Barcoded Medication Administration(BMA)/Medication Administration Workstations (MAW) (excluding small form factor computers on the BMA/MAW carts which have both clinical and administrative functionality and are therefore IT) VistA Blood Establishment Computer Software (VBECS), Intensive Care Unit (ICU), Clinical Information System (CIS),		X

Item Number	**Item Description**	**FUNDING SOURCE** IT Systems Account or Other Authorized Accounts/Funds	**FUNDING SOURCE** Accounts Other than those that fund IT
	Anesthesia Record Keeper (ARK), Medical Urethral System (MUSE), Laboratory, prescription, etc.). See Appendix B – Explanatory Notes 4 and 5.		
30	Dictation/Speech Recognition Systems requiring hardware/servers connected to VA network and software licenses. See Appendix B – Explanatory Notes 8 and 13.	X	X
31	Telemedicine Systems including Teleradiology, Telepathology, Telemental health, etc. (excluding video conferencing equipment, see Appendix B – Explanatory Note 6. (MCSEDS)		X
32	Copiers (Office Equipment).		X
33	Desktop Fax Machines - does not include software/server based faxing solutions. (Office Equipment)		X
34	Multi-function Device, as defined (Office Equipment).		X
35	Facilities Management Systems (Building Controls, Digital Signage, Energy and Elevator Control Systems, Fire Alarm Systems, Building security (i.e., Video Surveillance, Physical Access Control, Alert Notification Systems etc.), energy efficient lighting monitors (see Appendix B – Explanatory Note 7). (Facility Equipment)		X
36	Satellite Communications (dishes/uplinks).	X	
37	Diagnostic Workstations (i.e., Radiology, Cardiology, Pathology) (MCSEDS).		X
SOFTWARE			
38	Interfaces, Middleware. See Appendix B – Explanatory Note 5.	X	
39	Clinical Decision Support System (CDS) - see Appendix B – Explanatory Note 5 (MCSEDS)		X

Item Number	**Item Description**	**FUNDING SOURCE** IT Systems Account or Other Authorized Accounts/Funds	**FUNDING SOURCE** Accounts Other than those that fund IT
40	Clinical Information System (CIS) - see Appendix B – Explanatory Note 5. (MCSEDS)		X
41	Operating Systems (Note: OS for medical device data systems are funded from accounts other than those that fund IT)	X	
42	Diagnostic Tools. (See Appendix B – Explanatory Note 9)	X	
43	Cyber and Information Security Tools.	X	
44	Office Automation (i.e., Acrobat, Illustrator, Creative Suite, OrgChartPro, staff scheduling etc.).	X	
45	Direct Medical Diagnostic or Treatment Systems - Bio-Medical Systems Software (OR, ICU, PACU, ED, Radiology, etc.) and Stand-Alone Software used for direct patient care, excluding VA developed. See Appendix B – Explanatory Note 8 and 10 (MCSEDS)		X
46	Core Information Systems (VistA, VI, Exchange, Vetsnet, HDR, etc.).	X	
47	Electronic Media Subscriptions which require no software licenses.		X
48	Software as a Service (SaaS). See Appendix B – Explanatory Note 11.		X
49	Platform as a Service (PaaS). See Appendix B – Explanatory Note 11.	X	
50	Infrastructure as a Service (IaaS). See Appendix B – Explanatory Note 11.	X	
51	All software licenses, enterprise and unique, except for biomedical and clinical software. See Appendix B – Explanatory Note 5.	X	
52	USA Staffing: a web-based HR assessment tool Subscription Service which requires no software licenses.		X
53	Real Time Locator System.		X
54	Cloud Environment Development or Acquisition and General Support Services	X	

Item Number	**Item Description**	**FUNDING SOURCE** IT Systems Account or Other Authorized Accounts/Funds	**FUNDING SOURCE** Accounts Other than those that fund IT
55	Purchase or migration of IT required funded applications to a cloud environment.	X	
56	Purchase or migration of applications funded from accounts other than those that fund IT to a cloud environment.		X
57	Commercial-Off-The-Shelf Software for Direct Patient Care meeting criteria in section 2.c. of this directive.		X
58	Commercial-Off-The-Shelf Software NOT for Direct Patient Care not meeting criteria in section 2.c. of this directive.	X	
Other			
59	Major/Minor/NRM/Station Projects (Excluding Activation). See Appendix B – Explanatory Note 12. (Construction Projects)		X
60	Maintenance Contracts for IT-funded Hardware and Software.	X	
61	Microsoft Enterprise Licenses for Windows, Office, SMS, SQL, Exchange.	X	
62	Cisco SmartNet Maintenance Contract.	X	
63	VistA Maintenance & Expertise Center (VMEC)/VistA Imaging/Exchange.	X	
64	Telecommunications Costs (Voice, Data and Video, both Local service and long-distance telecommunications and telephony usage charges.) Telecommunications infrastructure (i.e., circuits and switches, wired cabling to the wall), regardless if the space is VA owned or leased.	X	
65	Release of Information (ROI) Software Maintenance.	X	
66	Quality Enhancement Research Initiative (QUERI). (MCSEDS)		X
67	Supply Fund Purchases of IT		X

Item Number	**Item Description**	**FUNDING SOURCE** IT Systems Account or Other Authorized Accounts/Funds	**FUNDING SOURCE** Accounts Other than those that fund IT
	items/services for own use are not to be included in the IT systems appropriation.		
68	Franchise Fund purchases of IT items/services for own use are not to be included in the IT systems appropriation.		X
69	All IT costs in support of VA mission-related operations incurred by VA Franchise Fund Enterprise Centers under OIT management.	X	
70	IT Managed Services (except for SaaS and Vendor Managed Services for the Business).	X	
71	IT Shared Services.	X	
72	Web Development and Infrastructure.	X	
73	Web **Content** Development, Management and Services.		X
74	Simulation equipment and programs used for clinician training.		X
75	Veterans Canteen Service (VCS) - IT support that is provided to other components of VA and is not specific only to VCS, such as use of VA network servers and installation and maintenance of security software.	X	
76	Veterans Canteen Service (VCS) – Costs that are specific only to VCS or VCS operations.		X
77	Compensated Work Therapy (CWT).		X
78	Printing and Reproduction.		X
79	IT system administration training.	X	
80	IT development and testing environments and performance testing.	X	
81	IT life cycle planning, technical requirements gathering (not business requirements) and definition and evaluation as necessary and incidental to the development, acquisition and operation of IT systems.	X	

Item Number	**Item Description**	**FUNDING SOURCE** IT Systems Account or Other Authorized Accounts/Funds	**FUNDING SOURCE** Accounts Other than those that fund IT
82	End User Support Center operations for IT capabilities operated by VA.	X	
83	Applications end-user business process re-engineering.		X
84	Leased space or non-VA furnished space occupied only by OIT employees whose salaries are paid by the IT Systems appropriation, not to include new construction.	X	
86	Initial costs of IT-related assets and services funded by non-VA grants or other non-VA funding sources, such as research efforts.		X
87	IT-related assets for delivery to Veterans provided by benefits programs under Title 38 authorities.		X
88	Veterans/Guest Internet Access (Guest Wi-Fi).		X
89	Patient Disposable Phones.		X
90	Costs of Background Investigations.		X
91	Cloud Credit-Non-VA Cloud Services using non-VA appropriated funding only (i.e., grant funding) for VA Medical Research.		X
92	Wi-Fi (Used in VA Operations by VA Staff & Contractors).	X	

APPENDIX B: EXPLANATORY NOTES

1. IT references all requirements/acquisitions funded with IT Systems account or other authorized accounts (see section 2b1 for various funding sources).

2. IT-related references all requirements/acquisitions funded from accounts other than those that fund IT, identified under OMB's Specialized Information Technology and Telecommunications Product Service Codes, Appendix B, regardless of dollar amount and includes interagency acquisitions of IT/IT-related requirements.

3. Other assets and resources reference all requirements/acquisitions for assets and resources that have a technology component that are not identified under Specialized Information Technology and Telecommunications Product Service Codes, Appendix B, regardless of dollar amount.

4. If the hardware is dedicated to solely running MCSEDS or Facility Software, it can be funded by accounts other than those that fund IT. If the hardware is used for both clinical and administrative functionality, then the MCSEDS /Facility Equipment software can be funded by accounts other than those that fund IT, but the hardware is funded by the IT Systems account or other authorized accounts or Funds. However, mobile computing devices that are predominantly involved in running MCSEDS applications for use in direct patient care must be funded by accounts other than those that fund IT (generally the Medical Services account). If the hardware solely runs administrative software, then the hardware is funded by the IT Systems account or other authorized accounts or Funds. (See Section 2. Policy)

5. Medical devices and equipment that communicate with VA IT networks must be funded by accounts other than those that fund IT if they can be categorized as MCSEDS in section 2.c. Systems that provide the administrative support of clinical/MCSEDS systems are funded by the IT Systems account or other authorized accounts or Funds. VA developed interfaces for items funded by accounts other than those that fund IT (MCSEDS) are IT. Vendor supplied interfaces, or upgrades to commercially produced software products with MCSEDS software are funded by accounts other than those that fund IT. Software operations and maintenance costs related to an acquisition funded by accounts other than those that fund IT are not funded through IT, including costs to transfer to a cloud environment.

6. Telemedicine modalities exclude videoconferencing equipment unless the videoconferencing equipment is exclusively used for patient care communications in real time (MCSEDS), in which case it is funded by accounts other than those which fund IT. The endpoint is defined as the Codec which is an IT expense. All peripherals (mouse, keyboard, PIV reader, bar code readers, monitors, speakers, microphones, headphones, headsets, etc.) attached to the Codec are not an IT expense.

7. Facility equipment must be funded by accounts other than those that fund IT; however, VA developed interfaces for Facility Management items must be

funded by an IT system account. Vendor supplied interfaces, or upgrades to commercially produced software products, with Facility Management software are funded by accounts other than those that fund IT but must comply with all VA IT standards. Software maintenance procured as part of an acquisition of Facility Management software is also funded by accounts other than those that fund IT.

8. All VA developed software costs will be considered IT; the development, acquisition, product support and management of software applications, including any open source, innovation, pilots, mechanisms and services for providing access to applications (i.e., mobile app store) in any IT environment operating under VA control. Purchased Commercially available off-the-Shelf (COTS) software that meets the definitions/criteria in section 2.c (MCSEDS) is funded by accounts other than those that fund IT; this includes acquisition, licensing and maintenance costs for this MCSEDS software; even if it is not FDA regulated; even if it is run on a standard PC or server.

9. This excludes diagnostic tools used exclusively to maintain (MCSEDS) items funded by accounts other than those that fund IT, which would be non-MCSEDS or systems used to maintain facility equipment; this is facility equipment (see Explanatory Note 7).

10. Mobile medical applications and associated devices are funded by accounts other than those that fund IT if they meet criteria defined under MCSEDS section 2c.2g. This includes the time to develop the application and integrate with the device, prior to it being placed into production usage. Associated data service (data plan) is also funded by accounts other than those that fund IT.

11. Software as a Service (SaaS) as defined by this policy in accordance with the National Institute of Standards and Technology's (NIST) guidelines (i.e., cannot be hosted on the VA network and no software can be downloaded from the service provider) are funded by accounts other than those that fund IT. Due to variants in SaaS offerings from industry, all funding request for SaaS projects must follow the SaaS approval process in Appendix C of this directive. Other service models used in VA's IT production environment such as infrastructure- (IAAS), platform- (PAAS) and telecommunications-as-a-service, as defined by National Institute of Standards and Technology's (NIST) guidelines, which require VA maintenance and/or interfaces to VA IT production environment, applications or data stores are IT.

12. Including modifications to a building's infrastructure, even though required specifically for IT purposes. Examples include: the acquisition and installation of a wire closet fiber optic infrastructure, power surge protection, distribution and battery backup systems and heating, ventilation and air conditioning (HVAC) equipment to comply with either operating requirements and/or manufacturer warranties. This includes construction of data centers. The IT Systems appropriation does not have the legal authority to incur any construction costs.

13. Dictation/speech recognition meets criteria delineated in MCSEDS section 2.c.(2) are funded by accounts other than those that fund IT; even if it is not FDA regulated or it is installed on VA IT networked devices. For example: PowerScribe and Voicebrook.

APPENDIX C: ACQUISITION AND MANAGEMENT OF VA INFORMATION TECHNOLOGY PROCESSES

For specific questions concerning the proper funding for IT items/services please refer to the below linked documents:

1. IT Workgroup (ITW) portal includes:

    a. Process Charter and Policy VA Directive 6008.

    b. Intake request page.

    c. User guide for intake process, for submission to ITW members.

    d. Meeting minutes and agendas.

    e. Decisions and related documentation.

    f. LINK:https://dvagov.sharepoint.com/sites/VHAITRMITFMOS/SiteAssets/ITNONITV 2/ITNonIT.aspx

2. Software as a Service (SaaS) and Cloud Services Request Process:

    a. SaaS requests must go through Unified Intake/Virtual Incident Procurement process (VIPR). The submission of the SaaS Inquiry Form (https://vaww.oit.va.gov/services/saas/) starts the process. This allows users to engage early in the process to talk with Digital Transformation Center (DTC) team to determine if something is SaaS (or not) and determine next steps. All requests will need to have a VIPR ID to progress through the process. VIP Request (VIPR) for SaaS starts the process moving through the VASI and authority to operate (ATO) process.

    b. All Cloud Services' requests must go through VIPR and have a VIPR ID to progress through the process. VIPR routes Cloud Services requests funded by accounts other than those that fund IT to the Account Management Office (AMO). AMO, ESCO and ITW representatives (as needed) validate applicability. All validated ECSO/VAEC Cloud Services requests funded by accounts other than those that fund IT will be routed to ECSO through the VA Enterprise Cloud site: https://dvagov.sharepoint.com/sites/OITEPMOECSO

3. Federal Information Technology Acquisition Reform Act (FITARA) Review Process:

    a. A FITARA Review is required for all requirements with IT related capabilities, regardless of funding appropriation, funding source and dollar value. The review is conducted in the Budget Tracking Tool (BTT) under the Acquisition Review Module (ARM) which expands the CIO's accessibility and visibility on IT procurements in accordance with FITARA. For more information on ARM, contact the Office of Strategic Sourcing at: Ask Strategic Sourcing