

VA SYSTEMS INVENTORY

1. **REASON FOR ISSUE:** This directive establishes the Department of Veterans Affairs (VA) Systems Inventory (VASI) as the authoritative source for VA Information Technology (IT) Systems and related system architecture information. This directive defines the purpose, criteria, roles and responsibilities for the use, management, and sustainment of VASI. Implementation of this policy is necessary to enable accurate assessment of current capabilities, prevent and remediate duplicative functionality and facilitate future planning resulting in efficient and effective use of VA resources. Except for the VA Office of the Inspector General, compliance with this policy is mandatory for all VA offices with responsibility for IT solutions that meet the VASI system characteristics described herein.
2. **SUMMARY OF CONTENTS/MAJOR CHANGES:** This directive:
 - a. Updates capabilities and functions of the VASI.
 - b. Updates/Identifies roles and responsibilities of stakeholders for systems registered in VASI.
 - c. Updates VA organizational roles and responsibilities regarding the use and management of VASI and the information contained within. Additions include Agile Center of Excellence (ACOE), Technology Business Management (TBM), VA Enterprise Cloud (VAEC), Architecture and Data Management Committee (ADMC), Standards & Architecture Council (SAC), Data Governance Council (DGC) and any subsequent offices performing stated roles and/or responsibilities.
 - d. Clarifies the role and purpose of VASI as distinct from other VA IT Asset and Inventory tools that manage software and hardware assets.
 - e. Ensures that VASI incorporates and aligns with the security accreditation boundary inventory documented in VA's Governance, Risk and Compliance Tool (VA GRC Tool).
3. **RESPONSIBLE OFFICE:** Office of Information and Technology (005).
4. **RELATED HANDBOOK/DIRECTIVE:** VA Directive 6051 Department of Veterans Affairs (VA) Enterprise Architecture (EA).
5. **RESCISSION:** VA Directive 6404 VA Systems Inventory dated February 23, 2016.

Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6404
Transmittal Sheet
April 28, 2026

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

A handwritten signature in black ink, appearing to read 'P. Lawrence', with a long horizontal flourish extending to the right.

Paul R. Lawrence, Ph.D.
Deputy Secretary of Veterans Affairs
Performing the Delegable Duties of the
Assistant Secretary for Information and
Technology and Chief Information Officer

DISTRIBUTION: Electronic Only

VA SYSTEMS INVENTORY (VASI)

1. **PURPOSE:** This Directive, in accordance with [Federal Information Security Modernization Act of 2014](#) (Public Law 113-283; December 18, 2014) and [OMB Circular No. A-130, "Managing Information as a Strategic Resource"](#), establishes the VASI as the authoritative reference inventory for VA's Information Technology (IT) solutions. VASI is a vital component of VA's Enterprise Architecture (EA) and is intended for use by internal VA users. VASI also provides users with a comprehensive view of VA's current IT solutions portfolio as well as tools enabling analysis and decision support across a wide variety of VA EA topics.

This directive enables the Department of Veterans Affairs to:

- a. Maintain an accurate reference inventory describing VA IT solutions and related metadata.
- b. Provide a standard definition of VA IT solutions and key system-related terms.
- c. Facilitate validation and management of the descriptive information captured over the life of a VA IT solution and enable search and discovery of related information.
- d. Align business capabilities and functions from the VA Business Reference Model (BRM) to the VA IT solutions that deliver them.
- e. Document the relationships between VA IT solutions and other contextual information (e.g., VA strategies, objectives, performance metrics, organizations, people, business capabilities, business functions, technical infrastructure, hardware, software, investments, data interfaces and exchanges and security data).
- f. Deliver an integrated view of VA IT solution information including data residing in other enterprise repositories.
- g. Provide timely VA IT solutions to VA leadership that improves decision support capabilities including planning, enhancement, retirement, and acquisition processes.
- h. Ensure alignment of the VA IT solutions registered in VASI with the Office of Management and Budget (OMB) reportable investment structure to improve accuracy, effectiveness, and efficiency of reporting to external stakeholders [i.e., OMB, Government Accountability Office (GAO), Office of Inspector General (OIG)].

- i. Ensure the VA IT solutions registered in VASI are compliant with all external Federal policies including, but not limited to, Federal Information Technology Acquisition Reform Act (FITARA) and OMB Circular A-130.
- j. Ensure alignment of VA IT solutions registered in VASI with the IT Product Line Management (PLM) framework to improve accuracy, effectiveness, and efficiency of system-centric reporting.
- k. Ensure alignment of the VA IT solutions registered in VASI with the Technology Business Management (TBM) Cost Transparency Model, to support Total Cost of Ownership (TCO) reporting.
- l. Ensure alignment of the VA IT solutions registered in VASI with the Configuration Management Database (CMDB) to support Service Configuration Management.
- m. Ensure alignment of VA IT solutions registered in VASI with VA's Governance, Risk and Compliance Tool (VA GRC Tool) to align VASI with the Federal Information Security Management Act (FISMA) inventory.

2. POLICY.

- a. VASI is VA's authoritative reference inventory of VA IT solutions. VASI shall be bound by the same access procedures and specifications applicable to the overall integrated VA EA. VASI information is available to authorized VA users (employees and contractors) with access to the internal VA network.
- b. VASI shall provide, at a minimum:
 - (1) VA-wide visibility of the registered VA IT solutions including system attributes, dependencies, capabilities, a description of the underlying IT technologies, and descriptions of any inter-dependences with non-VA IT solutions.
 - (2) Enabling functionality for the ease of users to register systems and update attributes.
 - (3) Tools enabling reporting and visualization of VASI data.
 - (4) Application profile information to support TCO reporting for VASI records, which are used as the lowest level of cost in the TBM Cost Transparency Model.
 - (5) The minimum data fields required for registration of VA IT Solutions.
- c. All VA IT solutions that meet the VASI criteria as documented in the VASI Handbook must be registered in VASI at discovery if already in operation or prior to development/acquisition begins.

- d. VASI Directive and Handbook shall be reviewed annually for policy regulations and memoranda that may be enhanced.

3. RESPONSIBILITIES.

- a. **Assistant Secretary for Information and Technology** shall:
 - (1) Provide executive sponsorship for VASI to support the Administrations and Staff Offices in the delivery of mission and support capabilities.
 - (2) Re-assess responsibilities under this policy if any reorganization within OIT occurs.
- b. **Chief Architect, Architecture & Engineering Services (AES)** has the primary responsibility for the provision and management of VASI. **AES** shall:
 - (1) Lead the overall implementation and management of VASI.
 - (2) Promote registration of all VA IT solutions to provide an authoritative view of the VA's current IT solutions portfolio.
 - (3) Review this directive and related handbook annually for any approved amendments.
 - (4) Provide training to promote the use of VASI through use case demonstrations of VASI capabilities and potential end user value.
 - (5) Provide requirements, design, development, engineering, maintenance, and the appropriate security compliance for the VASI tool used.
 - (6) Establish dashboards and reports to track system/product attributes for use in decision-making by IT leadership, portfolio directors, account managers, and product line managers. The current list of VASI attribute definitions and business rules can be accessed via the VASI website.
 - (7) Define and track metrics for VASI, including data accuracy, completeness, and its impact on execution level decision-making processes.
 - (8) Work with the Operations and Portfolio Management Committee (OPMC) to align portfolios and product lines to VA IT solutions.
 - (9) Integrate VASI with automated tools and workflows to streamline validation, reporting, and metadata updates for all registered VA IT solutions.
 - (10) Work with the VASI IO to align internal and external interfaces, to include, but not limited to Application Programming Interfaces (APIs), Graphical User interfaces (GUI), etc to VA IT solutions in VASI.

- (11) Co-chair and joint facilitate the Unified System Registry Work Group (USR WG) with VA GRC Tool under the Office of Information Security for Governance, Risk, and Compliance (GRC) Intake; and Cybersecurity Support for Information System Security Officers (ISSO).
- (12) Govern the maturation and increased quality of VASI content.
- (13) Develop and maintain a taxonomy and guidelines for categorizing and registering all VA IT solution technology and software components within VASI.
- (14) Assist VASI Information owners with the validation of their assigned VA IT solutions data in VASI and the data validation process to improve usefulness and compliance with data call requirements.
- (15) Assist VA IT solution owners with collecting original, planned, and updated date estimates for system development, deployment, implementation, and decommissioning for the IT modernization disposition status of systems registered in VASI.
- (16) Propose the appropriate business functionality (BRM alignment) of systems in VASI.
- (17) Refine, as necessary, the criteria for which VA IT solutions are required to be registered in VASI. VASI IT solutions criteria shall be documented and maintained on the VASI website.
- (18) Coordinate with other VA stakeholders on enterprise data management policies, governance, business processes, business and mission requirements, as well as on the implementation of Authoritative Data Sources (ADS) and VA IT solutions.

c. **Executive Director, Product Delivery Service (PDS)** shall:

- (1) Ensure any assigned VA IT solution that meets the VASI system criteria is registered in VASI.
- (2) Align assigned VA IT solutions registered in VASI to the correct portfolios and product lines.
- (3) Provide Application (APP) code alignment of VA IT solutions registered in VASI, if applicable.
- (4) Participate in USR WG to assist in system registrations, name changes and decommissions.
- (5) Use VASI to identify any assigned duplicative VA IT solutions.

- (6) Ensure assigned internal and external interfaces, to include, but not limited to Application Programming Interfaces (APIs), Graphical User interfaces (GUI), etc are aligned to an VA IT solution in VASI.
- (7) Participate in USR WG to assist with assigned VA IT solutions registrations, data updates, portfolio and product line alignment in VASI.
- (8) Identify assigned Business-Led IT systems (BLITS).

d. **Director, Office of Information Security (OIS)** shall:

- (1) Provide FISMA security accreditation boundary(s) and its alignment to VA IT solutions registered in VASI. FISMA boundary security compliance and authorization status are sourced from VA's Governance, Risk and Compliance Tool (VA GRC Tool). Data shall be integrated with VASI on a bi-weekly basis at minimum.
- (2) Ensure all security information is accurate and available for VA IT solutions registered in VASI.
- (3) Provide security guidance for VA IT solutions registered in VASI.
- (4) Participate in USR WG to assist in system registrations relevant to security updates.

e. **Deputy Chief Information Officer (DCIO), IT Budget and Finance (ITBF) and Chief Financial Officer, Office of Information and Technology** shall:

- (1) Provide alignment of both development and sustainment VA IT solutions registered in VASI to the proper IT investment code.
- (2) Confirm proper use of non-IT investments for VA IT solutions.
- (3) Confirm zero funding and expenditures for VA IT solutions planned for decommission.
- (4) Ensure alignment of VA IT solution names to Budget Tracking Tool (BTT) and OMB.
- (5) Ensure all project information aligned to VASI IT solutions is accurate.
- (6) Participate in USR WG to assist in VA IT solution registrations, data updates and alignments.

f. **Deputy Chief Information Officer (DCIO), Infrastructure Operations Services** shall:

- (1) Provide Veterans Affairs Enterprise Cloud (VAEC) product hosting location and hosting model alignment of VA IT solutions registered in VASI.
- (2) Confirm hosting and platform alignment for all VA IT solutions registered in VASI.
- (3) Confirm the shut down and sanitization of VA IT solutions determined to be decommissioned.
- (4) Provide Identity and Access Management (IAM) alignment to VASI registered VA IT solutions for two factor authentication (2FA) and Master Person Index (MPI) information.
- (5) Identify assigned Business-Led IT systems (BLITS).
- (6) Participate in USR WG to assist in VA IT solution registrations, data updates and alignments.

g. Deputy Chief Information Officer for Compliance, Risk, and Remediation shall:

- (1) Provide to VASI all required VA IT solutions stakeholders as identified in the Product Line Management (PLM) Transformation Playbook.
- (2) Participate in USR WG to assist in VA IT solutions registrations, data updates and alignments.

h. Director, Technology Business Management (TBM) shall:

- (1) Provide TBM alignment to VASI registered VA IT solutions.
- (2) Provide updates to the TBM model housed in VASI as needed.
- (3) Participate in USR WG to assist in VA IT solution registrations, data updates and alignments.

i. Chief Data Officer (CDO) shall:

- (1) Ensure VA's data strategy is implemented through the capture of VA data architecture related to VA IT solutions registered in VASI.
- (2) Identify and assign business data stewards, when appropriate, for each VA IT solution registered in VASI.

j. Operations and Portfolio Management Committee (OPMC) shall:

- (1) Provide the Portfolio and Product Line structure used in VASI.
- (2) Assign Portfolio Directors and/or Product Lines Managers.

- (3) Provides governance over Portfolio and Product Line changes.
- (4) Identify Business-Led IT systems (BLITS) in VASI.
- k. **Architecture and Data Management Committee (ADMC)** shall:
 - (1) Review recommendations provided by the Chief Architect for enforcement of this directive to conduct VASI related data calls.
 - (2) Collaborate with AES to monitor compliance with this directive, including the registration and governance of VA IT solutions and escalate issues to the SAC as needed.
- l. **Standards & Architecture Council (SAC)** shall:
 - (1) Review recommendations from the ADMC for approval.
 - (2) Enforce approved recommendations and recommend courses of action to rectify any related issues.
- m. **Data Governance Council (DGC)** shall: ensure that VA data management policies are consistent, and that VA IT solutions identified as Authoritative Data Sources (ADS) are identified within VASI.
- n. **Administrations & Staff Offices.** In execution of their mission responsibilities VA Administrations and staff offices shall:
 - (1) Confirm VASI registration for VA IT solutions supporting administration and staff office business capabilities or functions.
 - (2) Ensure VA IT solutions description, system criticality (a business perspective on impact of system failure), stakeholder information (e.g. business sponsor, and data steward), sponsor organization, VA capability, business function, business process, hardware/software mappings are accurate and current in VASI.
 - (3) Ensure VASI information is updated or validated during VA IT solution reviews no less than every 180 days.
 - (4) Support AES efforts to gather system Interface information to accurately reflect system dependencies and business transactions.
 - (5) Ensure compliance with this policy within decision and governance processes as appropriate.
 - (6) Identify Business-Led IT systems (BLITS) in VASI.
- o. **Key Stakeholders.** The VASI stakeholders listed below are required for each VASI system record. These stakeholders must be Government employees that

perform or oversee the responsibilities listed for each stakeholder role as follows:

- (1) **VASI Information Owner (VASI IO)** is the primary contact for information related to a VA IT solution registered in VASI (the VASI IO may or may not be the same as the Information System Owner (ISO) which is a role associated with a system's Authority to Operate (ATO) assigned in VA GRC Tool) and shall:
 - (a) Review, update, and validate assigned VA IT solutions with AES at minimum every 180 days.
 - (b) Approve VA IT solution updates submitted by additional stakeholders.
 - (c) Update the System Disposition Roadmap to reflect the future plans for the assigned VA IT solution across fiscal years and quarters.
 - (d) Update significant changes made to the stakeholder contact list, technology.
- (2) **AES Solution Architects** shall provide guidance to product teams to ensure compliance with VASI registration criteria, metadata standards, and enterprise alignment for VA IT solutions.
- (3) **Portfolio Director and Product Line Manager** shall have the overall management oversight responsibility to ensure system data is accurate and available for systems aligned to their Product Line(s).
- (4) **Business Owner** shall:
 - (a) Be responsible for the VA IT solution roadmap and how to convey the information within their VASI system record, including the description of the business capabilities the VA IT solution is delivering.
 - (b) Maintain ownership of the business capabilities and functions documented in VASI, including the primary business function associated with the VA IT solution.
- (5) **Data Stewards** shall: manage VASI-related data within their organization as well as the implementation of data governance, management of processes and authoritative data sources, and compliance with data policies within their Administrations/Staff Offices.

4. REFERENCES

- a. VASI Website: <https://vaww.ea.oit.va.gov/enterprise-architecture/va-systems-inventory/>

- b. VASI Glossary: <https://vaww.ea.oit.va.gov/enterprise-architecture/va-systems-inventory/vasi-glossary/>
- c. National Defense Authorization Act for Fiscal Year 1996 (NDA):
<https://www.congress.gov/bill/104th-congress/senate-bill/1124>.
 - (1) The Federal Acquisition Reform Act of 1996 is Division D of the NDA
 - (2) The Information Technology Management Reform Act of 1996 is Division E of the NDA
- d. eGovernment Act of 2002: <https://www.archives.gov/about/laws/egov-act-section-207.html>
- e. OMB Circular A-130 - Managing Information as a Strategic Resource:
https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf
- f. Federal Information Technology Acquisition Reform Act of 2014 (FITARA):
<https://www.congress.gov/bill/113th-congress/house-bill/1232>
- g. Federal Information Security Modernization Act of 2014 (FISMA):
<https://www.congress.gov/bill/113th-congress/senate-bill/2521>
- h. Federal Financial Management Improvement Act of 1996 (FFMIA):
<https://www.congress.gov/bill/104th-congress/house-bill/4319>
- i. OMB M-10-06, Open Government Directive, December 8, 2009:
https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2010/m10-06.pdf
- j. OMB M-12-18, Managing Government Records Directive, August 24, 2012:
https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2012/m-12-18.pdf
- k. President Executive Order, Making Open and Machine Readable the New Default for Government Information, May 9, 2013:
<https://www.govinfo.gov/content/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13642.pdf>
- l. OMB M-13-13, Open Data Policy- Managing Information as an Asset, May 9, 2013: https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2013/m-13-13.pdf
- m. VA Directive 6051, Enterprise Architecture, April 8, 2016:
https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=830&FType=2

- n. VA Directive 6500, VA Cybersecurity Program, February 24, 2021:
https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1254&FType=2
- o. VA Directive 0900, VA Enterprise Data Management (VADM), December 8, 2020: https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1218&FType=2
- p. VA Memorandum, Isolation Architecture for Networked Medical Devices (WebCIMS 453293):
https://vaww.va.gov/vhapublications/viewpublication.asp?pub_id=7535
- q. The Product Line Management Transformation Playbook, Version 3.1, August 2023:
<https://dvagov.sharepoint.com/sites/OITACOEPortal/Methodology/Key%20Changes/PLM-Transformation-Playbook-3.1.pdf>

5. DEFINITIONS.

- a. **Application (APP) Codes.** A billing code created by OIT Infrastructure Operations to track hosting and technical support costs used in multiple places across OIT. SOURCE: VASI Glossary
- b. **Application Programming Interface (API).** A communication interface with a well-defined syntax for methods that provide functionality and information from a software application, endpoint, or user code. SOURCE: VASI Glossary
- c. **Application Programming Interface (API) Standards.** As defined in OIT Directive 6700, API standards enable project teams to adapt to change, implement new capabilities, and reuse existing capabilities while ensuring appropriate data stewardship. In support of this purpose, documentation of APIs is required. It also requires development or updates of APIs and the corresponding data and services as appropriate. SOURCE: OIT Directive 6700
- d. **Authoritative Data Source.** A source of data or information designated as official source of data after recognition by the Data Governance Council and endorsement by the Chief Data Officer and is recognized as trusted, timely, and secure and is used within VA's information environment in support of VA business processes. Administrations and Staff Offices nominate these sources within domains for which they are the stewards. OIT develops and maintains technology solutions (e.g. services) that use these sources. SOURCE: VA Directive 0900
- e. **Business Data Steward.** The person is formally assigned and entrusted with accountability for business (non-technical) responsibilities. It is their responsibility to ensure effective control and use of data and information assets implemented. SOURCE: VA Directive 0900

- f. **Capability.** The ability to achieve a desired effect under specified performance standards and conditions through a combination of ways and means activities and resources to perform a set of activities. SOURCE: OIT Master Glossary
- g. **Capital Planning and Investment Control.** A systematic approach to selecting, managing, and evaluating information technology investments. CPIC is mandated by the Clinger Cohen Act of 1996 which requires federal agencies to focus on the results produced by IT investments.
- h. **Data Management.** The set of disciplines and techniques used to process, store, and organize data. Relevant to managing VASI as part of VA Data Strategy. SOURCE: VA Directive 0900
- i. **Enterprise Architecture (EA).** EA is a management practice focused on performance improvement through the alignment of strategic objectives, business needs, and information technology capabilities. EA identifies whether its resources are properly aligned to the agency's mission and strategic goals and objectives. EA is used to drive business decisions toward a more effective and efficient agency performance. SOURCE: VASI Glossary
- j. **Investment Code.** The distinct title of an entry or investment as it appears on a separate line in a fiscal budget. SOURCE: VASI Glossary
- k. **Product.** In the context of this directive this term definition is synonymous with system.
- l. **Product Line Management.** Indicates the level of involvement and Product Line control of the system decision-making as well as related resources. Allowable values for this attribute include: SOURCE: VASI Glossary
 - (1) **Actively Managed.** A product assigned to a Product line, where the Product Line Manager has fully accepted responsibility for the product AND has the authority to make decisions critical to the successful delivery of the product capabilities requested. SOURCE: VASI Glossary
 - (2) **Externally Managed within OIT.** A product assigned to a Product line where the Product Line Manager has NOT accepted responsibility for the product AND is not currently supporting the product, but another area within OIT is supporting the product. SOURCE: VASI Glossary
 - (3) **Externally Managed outside OIT.** A product assigned to a Product Line where the Product Line Manager has NOT accepted responsibility for the product AND no one in OIT is supporting the product. (Note that Products "Externally Managed Outside OIT" may still be consuming infrastructure resources and if so, this product will be assigned cost in the TBM Model in proportion to the amount of infrastructure they consume relative to Products in the other two categories.) SOURCE: VASI Glossary

- m. **Security Accreditation.** The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. SOURCE: VASI Glossary
- n. **System.** 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. (As it pertains to this directive, systems and products are synonymous.) SOURCE: VASI Glossary
- o. **VA IT Solution.** A VA IT Solution encompasses IT systems, platforms, web services, APIs, and other software components that contribute to VA's business and IT capabilities.
- p. **Unified System Registry Work Group (USR WG).** The USR WG's purpose is to support the oversight, implementation, and alignment of information systems, system boundaries, service maps, and processes. The USR WG serves as the official governance body that executes on the processes, procedures, registrations, reviews, and approvals for information systems, system boundaries, service maps, and processes within VA's environment, as well as overseeing functions and processes pertaining to VA's Governance, Risk and Compliance Tool (VA GRC Tool) and VA Systems Inventory (VASI) 1:1:1 alignment. Additionally, the Members of the USR WG are tasked with communicating pertinent system-specific information to their respective organization(s). SOURCE: Unified System Registry Technical Working Group Charter