Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6063
Transmittal Sheet
August 31, 2021

OPERATIONAL ANALYSIS OF VA INFORMATION TECHNOLOGY (IT) SYSTEMS

1. **REASON FOR ISSUE:** This directive establishes policy to ensure the Department of Veterans Affairs (VA) Information Technology (IT) systems undergo Operational Analysis (OA) on a regular, periodic basis to examine whether an IT asset in production continues to meet its intended objectives and yield expected benefits and for compliance and alignment with VA policy, rules, standards and capabilities as well as Federal requirements. This policy and its associated processes are necessitated by IT asset performance and fiscal accountability as well as integration and consistency across VA's information environment. To better serve our Veterans, VA requires systematic oversight and analysis of operational systems to ensure that they continue to meet the needs and strategic goals of the agency and its customers. OAs shall:

    a. Enhance ongoing visibility and monitoring of VA IT systems in production, particularly with respect to measuring system performance against cost, schedule and performance and value management goals, as well as whether investments in IT are continuing to meet business and customer needs.

    b. Inform and influence IT governance and investment decisions through reviewing and documenting IT systems and capabilities that are potential candidates for modernization, enhancement, replacement, or retirement.

2. **SUMMARY OF CONTENTS:** This directive shall:

    a. Establish the requirement for regular OA of VA IT systems in production for evaluation against regulatory guidance-based agency criteria and compliance with VA policy, requirements, rules, standards and guidance.

    b. Assign responsibility for OAs and actions resulting from systems determined to require remediation or replacement.

3. **RESPONSIBLE OFFICE**: Office of Information and Technology (OIT) (005), Development, Security and Operations (DevSecOps).

4. **RELATED HANDBOOK:** None.

5. **RESCISSION:** None.

Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6063
Transmittal Sheet
August 31, 2021

CERTIFIED BY:

/s/
Dat P. Tran
Acting Assistant Secretary for
Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Dominic A. Cussatt, CGEIT, CISM
Acting Assistant Secretary for
Information and Technology and
Chief Information Officer

Distribution: Electronic Only

OPERATIONAL ANALYSIS OF VA IT SYSTEMS

1. **PURPOSE AND SCOPE.** This directive establishes policy requiring regular, periodic Operational Analysis (OA) of Department of Veterans Affairs (VA) Information Technology (IT) systems in production as described in this directive. OA is a method of examining the ongoing performance of an operating asset and measuring that performance against cost, schedule **and** performance goals. OAs will assess IT systems that are in the production environment identified in the VA Systems Inventory (VASI), which according to Directive 6404 is VA's authoritative source for IT systems, against regulatory guidance-based agency evaluation criteria and requirements.

   VA IT systems are one of the key enablers in providing critical services to our Veterans. It is important for VA to have adequate visibility into the operational effectiveness of its IT systems in achieving VA's business objectives and operational and financial goals. Office of Management and Budget (OMB) Circular A-11, Capital Programming Guide identifies Operational Analysis as a key tool for monitoring operational assets and recommends that all agencies must manage IT assets and measure their financial, physical and operational condition for supporting the agency mission. This policy will enable the Department to accomplish the following:

   a. Ensure that VA IT systems are evaluated for customer satisfaction, strategic and business results and financial performance.

   b. Ensure VA IT Systems are effectively managed, integrated and maintained.

   c. Ensure that VA IT Systems are redesigned, modified, or decommissioned as appropriate.

   d. Provide requirements to the Planning, Programming, Budgeting and Execution (PPBE) process for development, modernization, enhancement, or sustainment IT funds necessary to ensure VA IT systems remain compliant/aligned with Federal and VA criteria, policies, rules and standards.

   e. Improve accuracy and efficiency of system-centric reporting by capturing and validating the current state attributes and performance of VA IT systems necessary for VA IT governance and leadership decisions.

   f. Promote responsible management of investments in IT and adherence to the select/control/evaluate model under both Government Accountability Office's (GAO's) IT Investment Management (ITIM) framework and OMB's Capital Programming Guide in which OA is a key practice.

2. POLICY.

a. VA must review, plan for and actively manage IT appropriated systems in production and apply effective measures of VA IT systems' financial and physical condition and operational support for the agency mission. This must be accomplished through the OA process, which applies once the first usable functionality of a system has been in the operational environment for at least twelve months.

b. All VA IT systems identified in VASI, VA's authoritative source for IT systems inventory per VA Directive 6404, that are in production will be subject to periodic OA reviews to ensure their continued alignment with VA policies, rules, standards and capabilities. Systems in production consist of existing operational systems (known as steady-state) and systems that are in both development and sustainment (known as mixed lifecycle).

c. All VA IT systems in VASI are prioritized by system criticality, which will be a determinant in planning OA reviews. Refer to the OA Process Guide for details.

d. OA assessments will be made against regulatory guidance-based agency evaluation criteria and will formally document and address cost, schedule and performance measures as well as areas of customer satisfaction/results, strategic and business outcomes, financial performance and innovation. OA results will be made available to decision-makers through a centralized repository.

e. All recommendations or issues of misalignment or non-compliance with VA IT policies determined through OAs will be escalated through OIT's current IT Governance channels for remediation and funding or waiver decisions.

f. Due to the Office of Inspector General's (OIG) statutory independence, including independent IT appropriation, requirements in this directive do not apply to OIG.

3. RESPONSIBILITIES.

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

(1) Advise and assist as requested to support OA of VA IT systems in production on any problems or questions of an administrative nature encountered during the implementation or operation of the program established by this directive.

(2) Designate appropriate business line liaisons to collaborate with OIT OA owners as necessary to enable OA of IT systems.

(3) Assist the CIO with review or resolution of escalated OA issues as requested within their business lines.

b. **In addition to the responsibilities above, the Assistant Secretary for Information and Technology/VA Chief Information Officer (VA CIO)** shall:

(1) Establish policy, processes and oversight to coordinate implementation and maintenance of this directive at the Department level.

(2) Develop, execute and monitor processes that enable OA of VA IT systems.

c. **Deputy Assistant Secretary (DAS) for DevSecOps, Deputy Chief Information Officers (CIOs) and Deputy Chief Information Security Officer (CISO)** shall:

(1) Ensure applicable VA IT systems owned by the OIT Directorate are reviewed against regulatory guidance-based agency defined evaluation criteria in accordance with the OA policy and process.

(2) Coordinate with the Operations and Portfolio Management Committee (OPMC) up to the Program and Acquisition Review Council (PARC) IT governance bodies to review and approve OA schedules, results and recommendations prior to any external reporting to OMB.

(3) Coordinate with the OIT Account Management Office (AMO) to remediate, resolve and/or obtain customer input on any customer impacts resulting from issues or recommendations identified through OAs and to inform PPBE processes accordingly.

d. **Office of Information and Technology Associate Deputy Assistant Secretaries (ADAS) and Executive Directors** shall:

(1) Submit OA issues and findings via the Operations and Portfolio Management Committee (OPMC) to the Program and Acquisition Review Council (PARC) through the appropriate OIT Directorate chain of command responsible for the system and its OA prior to external OMB reporting.

(2) Coordinate with appropriate stakeholders across VA to ensure that necessary remediation identified as part of OA reviews are planned, prioritized, funded and executed appropriately.

(3) Coordinate with OIT Directorates and IT Governance entities for portfolio management and adjudication of OA recommendations through enactment of investments and projects.

e. **Office of Information and Technology Directorates** shall:

(1) Each responsible OIT Directorate with ownership of applicable VA IT systems in VA's authoritative IT systems inventory shall identify and schedule for recurring review systems for which an OA is required. The schedule should be regularly refreshed to incorporate any additional systems in production.

(2) Each responsible OIT Directorate, as determined by Product Line and system ownership roles specified in VASI, shall assign responsible Sustainment Managers, Operations Managers, Project Managers, or appropriate equivalent personnel responsible for the system as OA owners to conduct OAs of systems covered by this policy. The responsible OIT Directorate shall designate the lead for accomplishing the OA and ensure that OA results are made available to decision makers through a designated centralized repository.

f. **Sustainment Managers, Operations Managers, Product Managers, or appropriate equivalent personnel** shall: conduct and document the system OA according to regulatory guidance-based agency defined OA evaluation criteria and the OA policy and process.

g. **Program and Acquisition Review Council (PARC)** shall:

(1) Review OA results and recommendations submitted via the Operations and Portfolio Management Committee (OPMC) by OIT Directorates with system ownership responsibility.

(2) Provide governance of investment, funding, sourcing and portfolio management decisions resulting from OA results and recommendations along with input from IT leadership, AMO and IT stakeholders.

4. REFERENCES.

a. 40 U.S.C. § 11101, Definitions and SUBTITLE III: Information Technology Management and The Clinger-Cohen Act of 1996

b. Federal Information Technology Acquisition Reform Act (FITARA): Title VIII, Subtitle D of the National Defense Authorization Act, P.L. No. 113-291

c. 44 U.S.C. Ch. 35, Information Resources Management

d. 44 U.S.C. Ch. 35, Federal Information Security Modernization Act of 2014, P.L. No. 113-283

e. Government Performance Results Act (GPRA) Modernization Act of 2010, P.L. 111-352, Jan 2011

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

g. OMB Circular No. A-130: Management of Federal Information Resources

h. Consolidated Appropriations Act, 2001, S-515, Information Quality Act (also known as the Data Quality Act)

i. OMB Memorandum M-15-14: Management and Oversight of Federal Information Technology (FITARA Implementation), June 10, 2015

j. OMB Memorandum M-12-18: Managing Government Records, Aug 2012

k. OMB Memorandum M-11-29: Chief Information Officer Authorities, Aug 2011

l. OMB Memorandum M-06-16: Protection of Sensitive Agency Information, June 23, 2006

m. GAO ITIM Framework for Assessing and Improving Process Maturity, Mar 2004

n. VA Directive 6500, VA Cybersecurity Program

o. VA Directive 6404, VA Systems Inventory (VASI)

p. VA Memorandum, *Categorization of Development, Modernization and Enhancements*, October 4, 2017

q. VA Office of Information and Technology, Program & Acquisition Review Council

r. VA Office of Information and Technology, Operations & Portfolio Management Committee

s. VA Office of Information and Technology, PPBE framework

t. VA Office of Information and Technology, VA Enterprise Architecture

u. VA Process Guide, *Operational Analysis, TBD.*

5. DEFINITIONS.

a. **VA IT System.** A VA Business Capability that: (1) Contains a combination of IT hardware, software, or information management capabilities; (2) Is funded via VA's IT appropriation and operationally managed by VA; (3) Is hosted in a shared computing environment (e.g., data center, cloud facility, medical center); (4) Is not an infrastructure or software sub-component (e.g., servers, network routers, storage) required to support a system and (5) Is not a Medical Device (e.g., cardiology equipment, medical lasers, endoscope) categorized under VA Medical Device Nomenclature System (MDNS).

b. **Operational Analysis.** Operational analysis (OA) is a method of examining the ongoing performance of an operating asset/investment and measuring that performance against an established set of cost, schedule and performance goals.

c. **Mixed lifecycle** refers to IT assets that are in both development and sustainment, i.e. have a portion or component in production.

d. **System Criticality Categorization.** Reference VASI Data Dictionary. Per VASI, System Criticality "defines the level of business criticality of a system in delivering the intended business capabilities. The levels include:

(1) Premium - Priority Systems with highest impact to delivering Veteran centric business capability.

(2) High - Systems that support critical business capabilities.

(3) Medium - Systems that provide non-mission centric business capabilities.

(4) Basic - Systems with lowest impact to delivering business capabilities."