
VA Enterprise Design Patterns:

6. Cloud Computing

6.1 Enterprise Cloud Services Broker

**Office of Technology Strategies (TS)
Architecture, Strategy, and Design (ASD)
Office of Information and Technology (OI&T)**

Version 1.0

Date Issued: November, 2015



THIS PAGE INTENTIONALLY LEFT BLANK FOR PRINTING PURPOSES

APPROVAL COORDINATION

Date:

Tim McGrail
Senior Program Analyst
ASD Technology Strategies

Date:

Paul A. Tibbits, M.D.
DCIO Architecture, Strategy, and Design

REVISION HISTORY

Version	Date	Organization	Notes
0.1	8/3/15	ASD TS	Initial Draft
0.3	9/22/15	ASD TS	Second draft with updates made throughout document based upon initial internal/external stakeholder review and comment.
0.5	10/19/15	ASD TS	Updated draft for stakeholder review prior to the Public Forum.
0.7	11/9/15	ASD TS	Final draft incorporating updates made following Public Forum.
0.9		ASD TS	Final version for TS leadership approval and signature, including all applicable updates addressing stakeholder feedback and Section 508 Compliance.

REVISION HISTORY APPROVALS

Version	Date	Approver	Role
0.1	8/3/15	Joseph Brooks	Enterprise Cloud Services Broker Design Pattern Lead
0.3	9/22/15	Joseph Brooks	Enterprise Cloud Services Broker Design Pattern Lead
0.5	10/19/15	Joseph Brooks	Enterprise Cloud Services Broker Design Pattern Lead
0.7	11/9/15	Joseph Brooks	Enterprise Cloud Services Broker Design Pattern Lead
0.9	11/17/15	Tim McGrail	ASD TS Design Pattern Final Review

TABLE OF CONTENTS

1	INTRODUCTION	1
1.1	BUSINESS NEED	1
1.2	APPROACH.....	1
2	CURRENT CAPABILITIES AND LIMITATIONS.....	1
2.1	LIMITATIONS	2
3	FUTURE CAPABILITIES.....	4
3.1	OPERATIONAL VISION	4
3.2	BUSINESS PRINCIPLES.....	6
3.3	TECHNICAL AND ARCHITECTURAL PRINCIPLES.....	7
3.4	SECURITY CONSIDERATIONS	8
3.5	NETWORK SECURE CONNECTION FRAMEWORK	9
3.6	FULL LIFECYCLE MANAGEMENT.....	10
3.7	ECSB SUMMARY	10
3.8	ALIGNMENT TO TECHNICAL REFERENCE MODEL (TRM).....	11
4	USE CASES	12
4.1	USE CASE ONE	13
4.2	USE CASE TWO.....	14
APPENDIX A.	DOCUMENT SCOPE	15
A.1	SCOPE.....	15
A.2	DOCUMENT DEVELOPMENT AND MAINTENANCE.....	15
APPENDIX B.	DEFINITIONS	15
APPENDIX C.	ACRONYMS.....	17
APPENDIX D.	REFERENCES, STANDARDS, AND POLICIES.....	19

FIGURES

Figure 1 - Conceptual TIC Architecture (From TIC 2.0 Reference Architecture).....	4
Figure 2 - VA ECSB Operational Concept (Based on materials provided by industry partners)	5
Figure 3 - Notional “To-be” VA ECSB	6
Figure 4 - Applying Agile Workflow Service Lifecycle Process (Based on materials provided by industry partners)	7
Figure 5 - FIPS 199 Standards for Classification of Federal Information and Information Systems	9
Figure 6 - High-Level Roadmap for Establishing an ECSB.....	11

Figure 7 - Overview of the NIST Cloud Computing Reference Architecture including a reference to the Cloud Broker capabilities 12
Figure 8 - User Provisioning Use Case..... 13
Figure 9 - Business Use Case (Provided by industry partners)..... 14

TABLES

Table 1 - Representative VA Tool Categories and Approved Technologies..... 11

1 INTRODUCTION

VA has invested in cloud computing at the project level, resulting in siloed capabilities without adequate governance and policies. In accordance with VA EA Vision and Strategy “To achieve VA transformation objectives, the supporting information environment must move from a disparate environment of stove-piped systems to a unified environment of integrated, interoperable business processes and technical services.” VA’s incorporation of cloud service providers (CSPs) supports the strategic goals of interoperable infrastructure, virtualized platforms/storage, and enterprise services in the Enterprise Technology Strategic Plan (ETSP). This Enterprise Design Pattern is the first increment that establishes architectural principles and constraints to inform enterprise solutions leveraging CSPs. This document establishes the requirement for an Enterprise Cloud Services Broker (ECSB) based on the National Institute of Standards and Technology (NIST) Cloud Computing Reference Architecture (NIST SP 800-292), and will align to all VA governance, policy documents, and mandated federal requirements.

1.1 Business Need

An ECSB supports all Lines of Business (LOBs) and the Office of Information and Technology (OI&T) in establishing a shared vision for managing the integration of Federal Risk Authorization and Management Program (FedRAMP) accredited CSPs for project-specific business needs. Projects will use the ECSB as a “one-stop shop” to discover, access, and integrate CSPs via collaboration with OI&T. The ECSB fosters collaboration among both business and IT stakeholders, and supports standardized solutions including approved enterprise resources hosted outside of VA regional data centers.

1.2 Approach

VA is establishing a long-term initiative for incorporating external CSPs to achieve objectives established in the Office of Management and Budget (OMB) “Cloud First” strategy and VA Directive 6517. VA’s cloud computing initiative, outlined in *A Strategy for VA Cloud Adoption*, stems from direction by OI&T senior leadership to evaluate criteria for adopting CSPs or migrating existing IT infrastructure to CSPs. The initiative accounts for lessons learned from previous implementations in the Federal Government and the private sector, and supports VA’s goal to achieve cost efficiencies while handling increased customer demands for enterprise services. Incorporating CSPs into the Enterprise Technical Architecture (ETA) hinges on establishing and using the ECSB to mediate CSP connections among diverse service consumers across VA.

2 CURRENT CAPABILITIES AND LIMITATIONS

As outlined in *A Strategy for VA Cloud Adoption*, VA has invested in numerous enterprise-wide cloud capabilities to facilitate developing and supporting new applications for each VA LOB.

These capabilities include the Enterprise Development Environment (EDE) at the Austin Information Technology Center (AITC), which provides a hosting environment that has virtualization capabilities associated with Infrastructure-as-a-Service (IaaS). VA also uses an outsourced private hosting environment provided by Terremark for key services including Veterans Relationship Management (VRM), Customer Relationship Management (CRM), Identity and Access Management (IAM), and VA Mobile Framework (VAMF). These hosting environments have satisfied functional requirements for many projects in the past, but they do not completely provide the rapid elasticity and on-demand self-service found in commercial CSPs.

Many projects are increasingly evaluating external CSPs to meet evolving business requirements, but integrating CSPs can be too complex for projects to manage themselves. A project-level cloud consumer may request services from the ECSB instead of contacting a CSP directly, enabling a single point access for integration, monitoring, and interoperability. The ECSB is an entity managing the use, performance, and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers. VA lacks an ECSB enabling LOBs to deploy, integrate, and maintain cloud services. *A Strategy for VA Cloud Adoption* identifies the following challenges to establishing an ECSB:

- Cloud initiatives conducted at the project level with no enterprise oversight
- Lack of a standardized process to evaluate CSPs to ensure compliance with FedRAMP and Federal Information Security Act (FISMA) controls, including appropriate connections with Trusted Internet Connection (TIC) access points managed by VA's Network and Security Operations Center (NSOC)

2.1 Limitations

Absence of Enterprise Cloud Office: VA has no single office to act as a gatekeeper for cloud adoption. VA Virtual Office of Acquisition (VOA) does not have a complete or searchable field providing an index of all current cloud environments. VA has twenty-six cloud environments registered in the acquisition office, with other cloud environments operating in silos.

Due to the lack of an ESCB, VA has the challenge of monitoring and overseeing all cloud initiatives without the centralized visibility an ECSB provides. These challenges exist due to the following:

- Requests for infrastructure lead to ad hoc and non-standard approaches
- No transparency/traceability – from requesting services to ongoing operations, utilization of services, financials, etc.
- No visibility into the resources available

- Non-compliance with VA Directive 6517: “Assisting and coordinating with VA information system owners in creating, maintaining and submitting cloud computing service change requests for continuous monitoring, implementation, or maintenance for approval to the Enterprise Security Change Control Board (ESCCB).”

Lack of agency-wide standards & initiatives: VA has not clearly defined policies to provision cloud using NIST SP800-53 and FISMA controls to determine the impact factor of a system.

The lack of a well-defined process for categorizing VA information security baselines and undefined terms leads to over-categorization:

- Policies and governance lack the appropriate set of rules to determine impact baseline controls as required by FedRAMP and Federal Information Processing Standard 199 (FIPS) for cloud computing security requirements baseline.
- Most VA systems are set at FedRAMP High Baseline.
- VA does not have a framework to evaluate and inherit the controls set by FedRAMP for Provisional Authority To Operate (PATO) cloud, which would allow vendors to gain full Authority To Operate (ATO) to work with VA using FISMA controls.
 - Operation Framework
 - Network secure connection framework
 - Data Security Framework and guidance
- VA media sanitation guides do not follow the latest NIST SP800-88 Rev 1, which permits cryptographic erase of logical volumes.
 - Current directive reflects information from prior NIST SP800-88

VA is not fully compliant with TIC 2.0 Reference Architecture, as it requires all external connections to be known and monitored.

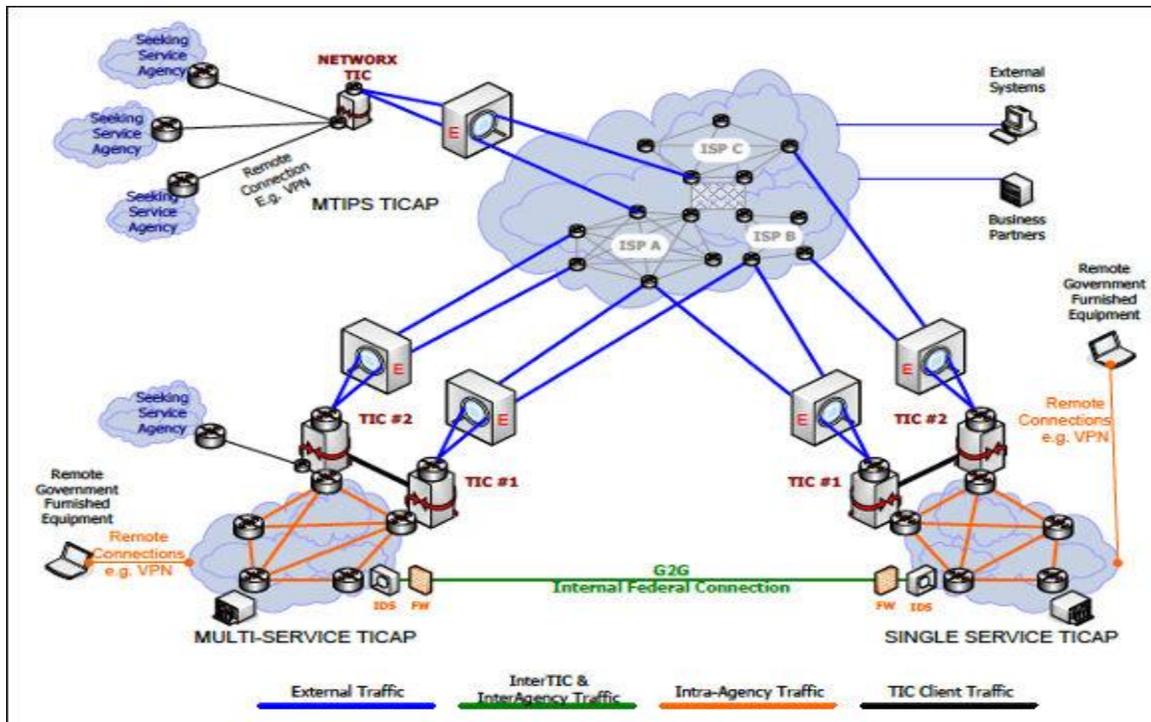


Figure 1 - Conceptual TIC Architecture (From TIC 2.0 Reference Architecture)

- VA's NSOC continues to implement the TIC initiative to identify all system interconnections and consolidate them into four VA gateways. Although there has been progress cataloging the many interconnections for monitoring purposes, unknown and unmonitored external connections still exist due to a lack of implementation standard security configuration baselines for all VA operating systems, databases, applications, and network devices.
- VA internally hosted cloud solutions (e.g., EO va.gov) create challenges in communicating with external entities inbound and outbound.

The following section provides architectural guidance supporting an enterprise-wide ECSB solution, enabling enterprise oversight in accordance with VA security policies regarding CSP integration. Cloud security and privacy requirements drive changes to VA Handbook 6500 and constitute a future Enterprise Design Pattern referenced in this document.

3 FUTURE CAPABILITIES

3.1 Operational Vision

VA needs to establish an ECSB with both technical and business functions to manage the use, performance, and synchronized delivery of cloud service offerings within VA, from other federal providers, and from commercial providers to sustain an integrated and controlled multi-cloud provider environment. As shown in Figure 2, the ECSB enables VA to tailor the availability and

delivery of cloud services based on technical and business requirements. The ECSB provides the single point for integrating this information from each of the CSPs, making it available to various VA and Government stakeholders – eliminating the need for each Administration to monitor CSP performance and security controls.

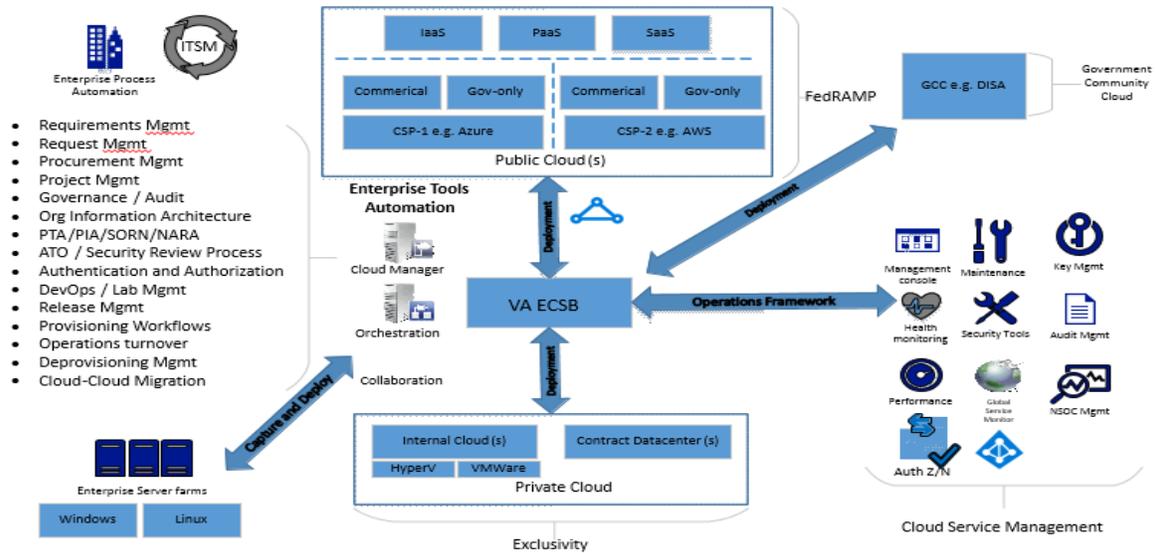


Figure 2 - VA ECSB Operational Concept (Based on materials provided by industry partners)

The ECSB will provide an integrated set of enterprise capabilities, including:

- Ensuring compliance with VA identity and access (IA) requirements for encryption and key management integration with VA’s IAM services
- Enabling integrated cyber intrusion detection and response
- Enabling a common entry into the cloud: VA cloud service provisioning catalog
- Providing an integrated billing and contracting interface with usage and cost management functionality down to the project level
- Managing integrated service delivery from VA and commercial service providers
- Providing integrated IA controls and integration with VA’s IAM services
- Controlling usage and optimizing cloud workload distribution
- Maintaining configuration control of VA resources deployed into the cloud
- Ensuring that providers maintain VA standards and architectural compliance
- Enabling continuous monitoring and reporting on performance of Service Level Agreements (SLAs) and IA controls
- Providing a common, integrated help desk

The “To-be” ECSB is elastic and agile to enable VA customers and organizations to tailor the set of available services and optimize the cloud performance as requirements and policies evolve.

3.2 Business Principles

Efficient Cloud brokerage cannot function without clear policy guidance codified into executable business rules. The codified business rules (templates, approval routing, etc.) are implemented as automated workflows. Automating the workflows will improve efficiency, timeliness of service delivery, and consistency of engineering patterns and security controls implementation. VA needs a framework to evaluate and inherit the controls set by FedRAMP for PATO cloud that allow vendors to gain full ATO to work with VA using FISMA controls.

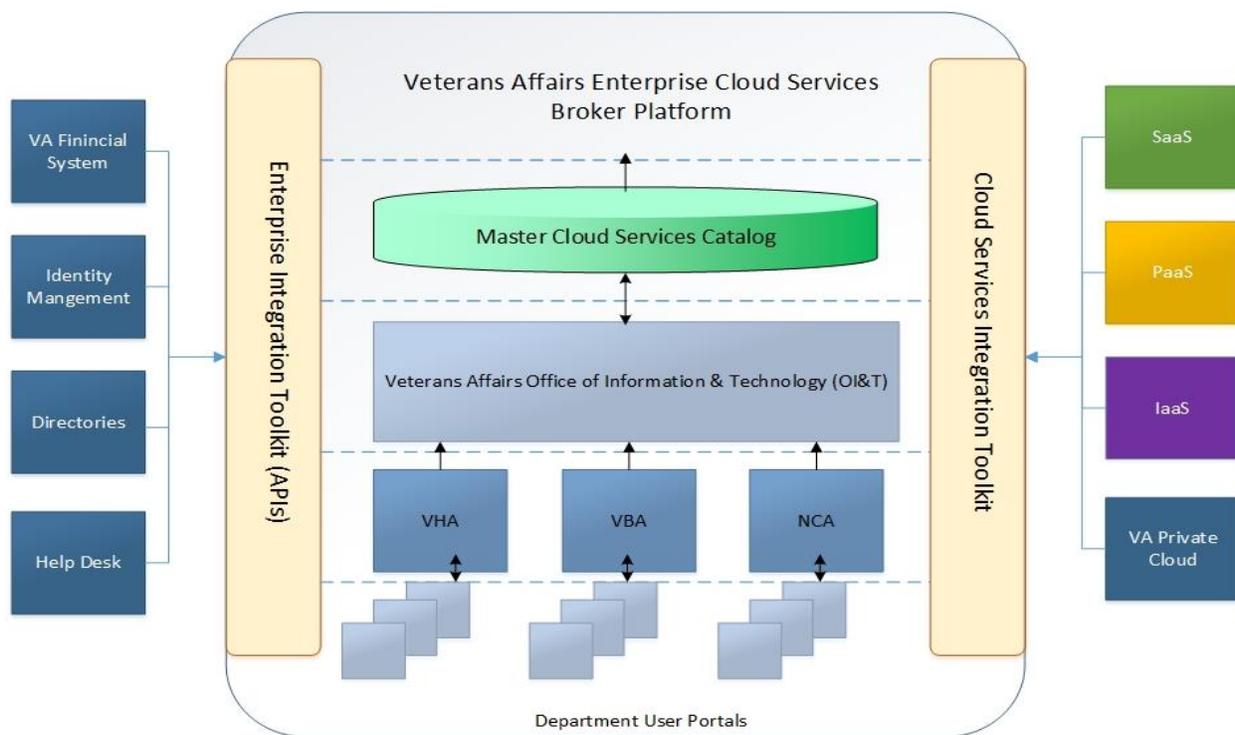


Figure 3 - Notional “To-be” VA ECSB

As shown by Figure 3, VA OI&T is mandating a robust governance framework and policies on cloud computing to ensure that the ECSB program aligns to the VA EA Strategy and Vision. This office will be responsible for creating the following templates:

- Acquisition package
- Business case
- Financial
- Procurement
- Contracting

- ECSB Cloud Strategies
- Relevant cloud adapting documentations according to VA cloud policy

As shown by Figure 4, each VA department submits business cases before gaining access to the VA ECSB platform.

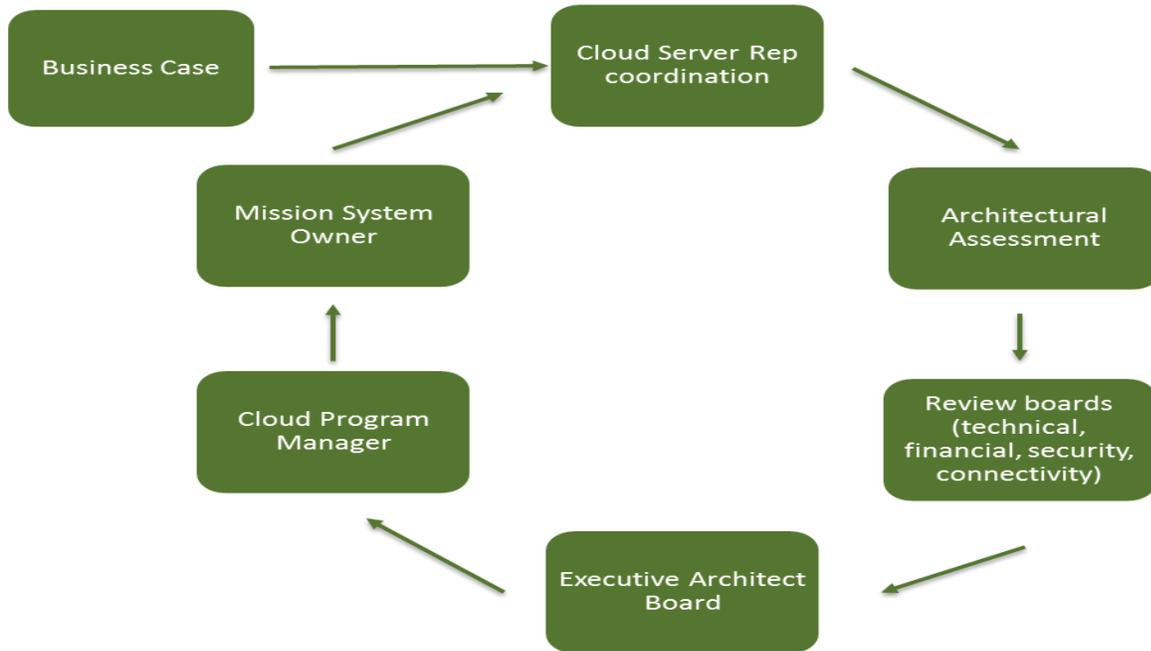


Figure 4 - Applying Agile Workflow Service Lifecycle Process (Based on materials provided by industry partners)

3.3 Technical and Architectural Principles

The technical concept for the ECSB “To-be” vision will enable business process automation and a cloud service management capability. The operational vision of the ECSB is similar to an application-programming interface (API) gateway for CSPs.

The guiding principles for the “To-be” ECSB are as follows:

- Consider open source platform (per VA Memorandum *Consideration of Open Source Software*, November 4, 2014) to facilitate innovative solutions and mitigate risks of vendor lock-in. Standards based approaches are recommended when open source is not feasible.¹

¹ At the time of publication, standards were not sufficiently mature to be a recommended approach. Unified Standards are in progress and still being defined across industries.

- Support transition of a largely on-premises IT infrastructure into a unified cloud environment with IaaS, Platform as a Service (PaaS), and Software as a Service (SaaS) capabilities managed and delivered through a single store front
- Provide VA users choice and self-service in a rapid fashion reducing provisioning time to market
- Ensure a foundation to scale beyond IaaS and PaaS to a broader catalog of SaaS

Required technical capabilities for the ECSB are as follows:

- Portal widgets used as interfaces for users and administrators
 - Plug-and-play widget concept
 - Allows for pre-built or custom service gateways
 - Allows for pre-built or custom broker portals or interfaces
- Cloud engine
- Fully customizable workflow management
- Broker widgets used as gateways to service providers for IaaS, PaaS, and SaaS
- An elasticity hybrid cloud platform to integrate with different cloud services, as shown in Figure 3

3.4 Security Considerations

The ECSB requires workflow templates to provision cloud resources according to data security in terms of Confidentiality, Integrity, and Availability (CIA) defined by NIST SP800 – 53 and NIST FIPS – 199 standards for classification of federal information and information systems as shown in Figure 5. The ECSB also provides the capability to support Privacy Threshold Analysis (PTA) before adopting new CSPs. The ECSB ensures compliance with the following standards:

- FISMA / FedRAMP LOW: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals
- FISMA / FedRAMP MODERATE: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals
- FISMA / FedRAMP HIGH: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

SECURITY OBJECTIVE	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals
Integrity Guarding against improper information modification or destruction, and includes ensuring information non- repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

Figure 5 - FIPS 199 Standards for Classification of Federal Information and Information Systems

3.5 Network Secure Connection Framework

The ECSB will ensure a secure network connection between VA environment and CSP. The ECSB will follow VA NSOC workflows to outline how the broker connects to send encrypted data through proper channels. These workflows will comply with the following federal policies:

- NIST SP800-67 Revision for Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
- FIPS Publication 197, Advanced Encryption Standard
- NIST SP800 – 88 Revision 1 for Guidelines for Media Sanitization

The ECSB will ensure operation with VA NSOC for network security. Before allowing live operation, NSOC will ensure the requirements listed below are enforced as outlined by FedRAMP-TIC Overlay (for mobile devices) and FedRAMP (for connection from Agency networks):

- Document how the FedRAMP security requirements are met
- Document how TIC capabilities for federal customers coming from an Agency network and supported alternatives for mobile users are met
- Undergo one combined assessment to demonstrate compliance with both FedRAMP and TIC
- Have the combined TIC / FedRAMP assessment be completed by a FedRAMP accredited 3PAO
- Achieve a FedRAMP security authorization by an authorizing official (agency or JAB) based on the Third Party Assessment Organization (3PAO) Security Assessment Report
- Be approved “TIC Ready” by DHS based on DHS’s review of a 3PAO TIC Capabilities Assessment Report

3.6 Full Lifecycle Management

The ECSB requires the capability to track system ownership across all CSPs. The ECSB defines the policies to manage the full capabilities and constraints of each cloud portfolio. This requires governance across the following areas:

- Cloud Portability: Ensuring applications can migrate among clouds over time (e.g. cloud bursting). These policies will eliminate the possibility of cloud lock in
- Cloud Interoperability – Ensuring policies to allow cloud data to migrate across multiple cloud platforms
- Service Health Management: Assure ultimate cloud optimization and Capacity Management for high performance of CSP and cloud resources
- Cost and Budget Analysis: Each cloud provider offers unique pricing models and options and different billing capabilities. Consider price models for “pay as you go” and longer term dedicated resources.
- SLA Compliance: Guidance and models to monitor continuous compliance with approved SLA for each CSP
- Audit Standards: Auditing standards and models should comply with NIST SP 800-92 for Guide to Computer Security and Log Management
- Provision Requirement: Ensure all CSP follow guidelines to provide standard API configurations out of box or clearly define the ability to support multi-tenancy
 - Define attributes for communication
 - Define role based control
 - Open source Software Transition Kit (STK)

3.7 ECSB Summary

- The ECSB provides the following opportunities to cloud service consumers: User experience versus administrative efficiency
- Security (due to using approved technologies in the TRM and FedRAMP-accredited CSPs)
- Providing a living marketplace versus an online portal
- Acquisition and Governance
- Managing the complex world of licensing—how to achieve a “single-swipe” approach
- Customer Outreach
 - Flexibility, Scalability, Adaptability
 - Expanding beyond IaaS
 - Integrating with external systems
 - Automating business processes for integrating with the CSPs

Figure 6 shows that the ECSB should provide:

- Operation Vision from all VA stakeholders
- Business and relationship support services (business intermediation)
- Technical support service (aggregation, arbitrage, and technical intermediation) with a key focus on handling interoperability issues among multiple CSPs
- Risk Management framework to support ECSB implementation

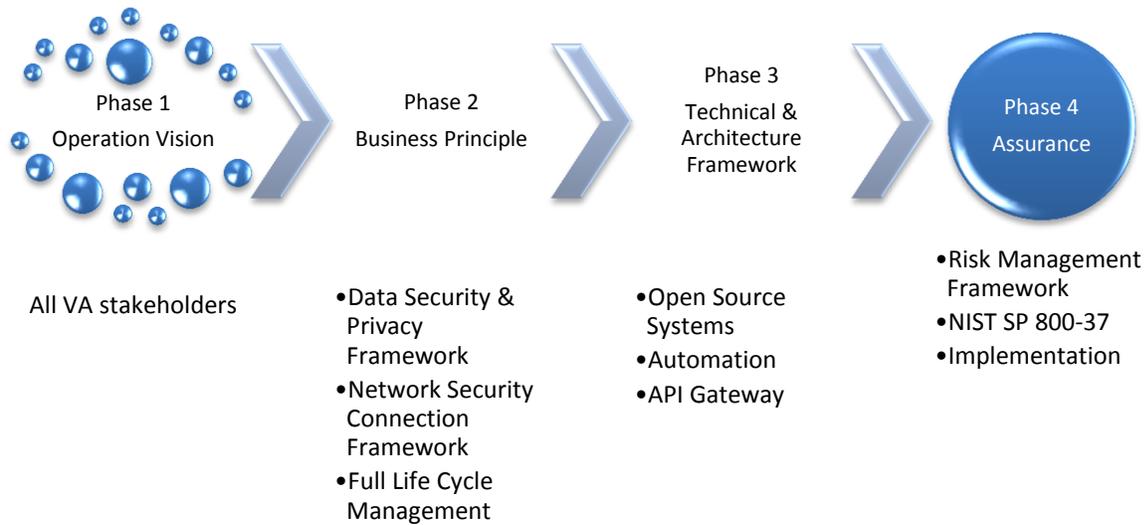


Figure 6 - High-Level Roadmap for Establishing an ECSB

3.8 Alignment to Technical Reference Model (TRM)

All projects will leverage the approved technologies and standards located in the VA Technical Reference Model (TRM). All approved CSPs will be included in the TRM and referenced in future versions of this document.

Table 1 - Representative VA Tool Categories and Approved Technologies

Tool Category	Example Approved Technologies
Cloud Technologies	CloudForms, EMC Atmos GeoDrive, iCloud, Heroku and OpenShift Enterprise
Virtualization Software	Citrix XenApp, Docker, Linux Containers,

	IBM WAVE for z/VM, VMware Tools and VirtualBox
Miscellaneous	Atlantis USX, HP Command View EV A, PhoneView, Tivoli Storage Manager for Space Management and Veritas Enterprise Administrator
Physical Servers	Servers, TSPrint
Data Center Automation Software	BMC Application Automation and Microsoft Center Operation Management

4 USE CASES

The ECSB represents three use cases in the NIST Cloud Computing Reference Architecture (NIST SP 500-290) as follows:

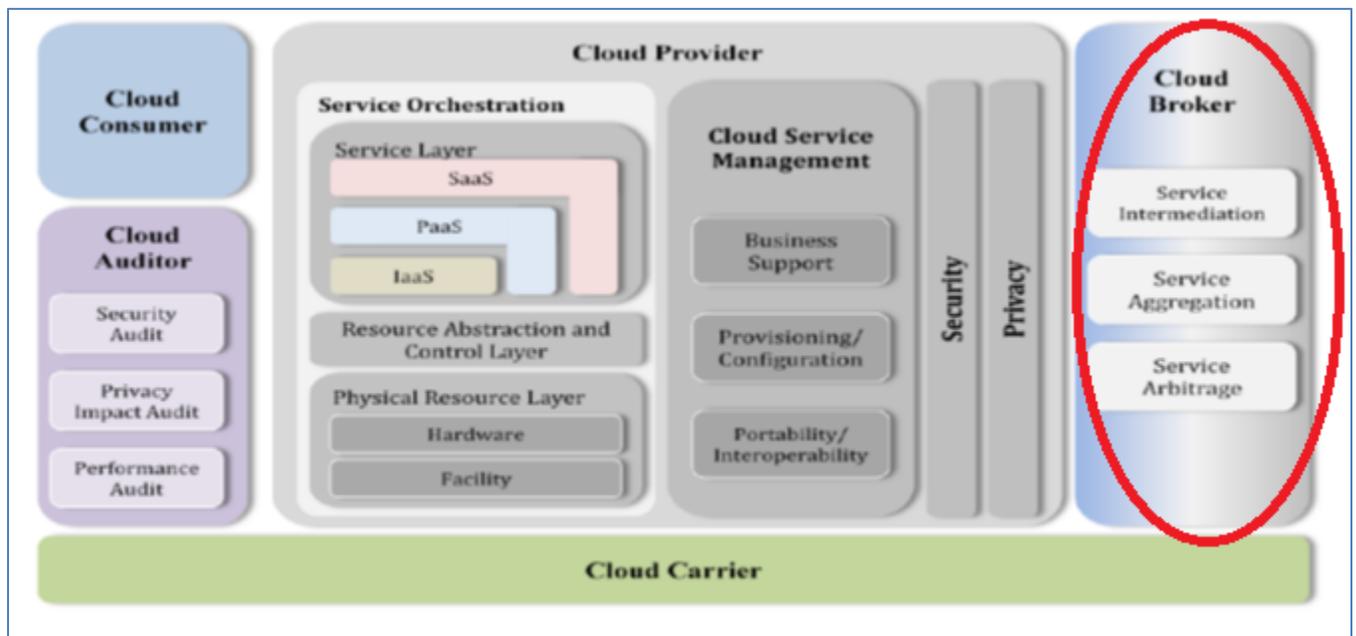


Figure 7 - Overview of the NIST Cloud Computing Reference Architecture including a reference to the Cloud Broker capabilities

The ECSB provides support for the following use cases per NIST SP 500-292:

- **Service Intermediation:** A cloud broker enhances a given service by improving a specific capability and providing value-added services to cloud consumers. The improvement can be managing access to cloud services, identity management, performance reporting, enhanced security, etc.

- **Service Aggregation:** A cloud broker combines and integrates multiple services into one or more new services. The broker provides data integration and ensures the secure data movement between the cloud consumer and multiple cloud providers
- **Service Arbitrage:** Service arbitrage is similar to service aggregation except the services are not fixed. Service arbitrage means a broker has the flexibility to choose services from multiple agencies. The cloud broker, for example, can use a credit-scoring service to measure and select an agency with the best score

NIST defines the ECSB in terms of a Business Broker and a Technical Broker. The Business Broker provides business and relationship services, and does not have any contact with the consumer’s data, operations, or artifacts (e.g., images, volumes, firewalls) in the cloud. Conversely, a Technical Broker does interact with a consumer’s assets by aggregating services from multiple cloud providers and adding a layer of technical functionality by addressing single-point-of-entry and interoperability issues. These broker roles are not mutually exclusive. For example, a given entity might serve as a Business Broker in one context, a Technical Broker in another, and both in a third context.

4.1 Use Case One

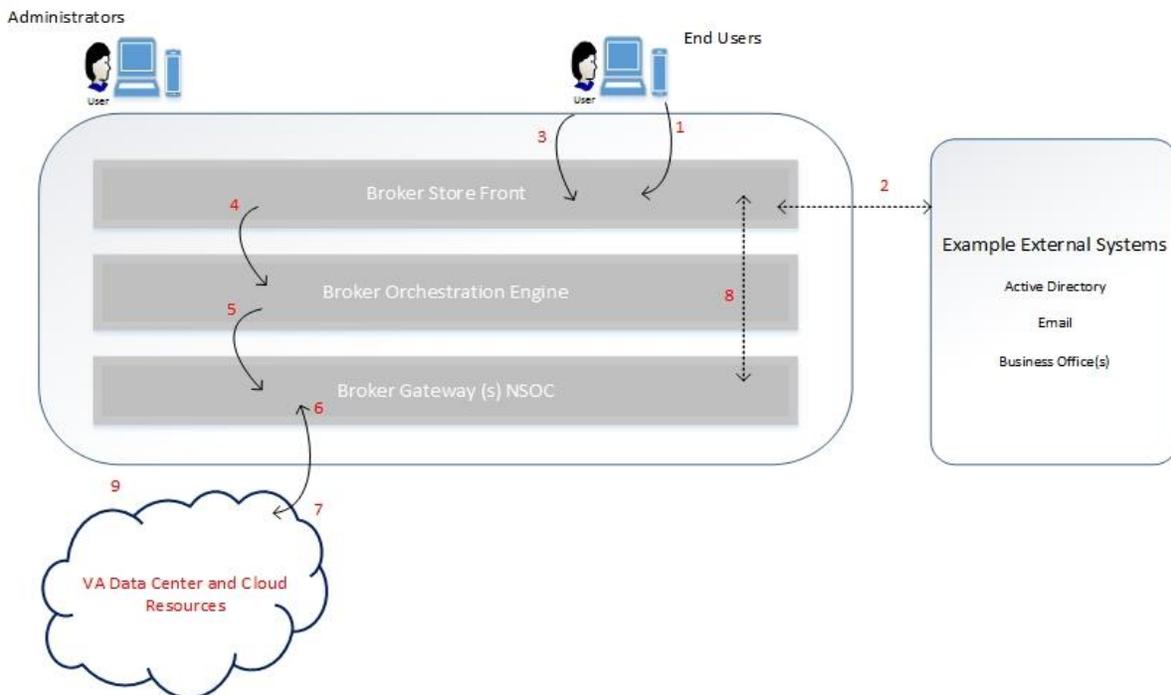


Figure 8 - User Provisioning Use Case

- 1) User accesses Storefront and provides credentials
- 2) Storefront verifies user’s identity

- 3) The authenticated user browses catalog and builds a shopping cart of services, submits order
- 4) Storefront validated quota and sends service request to Orchestration Engine
- 5) Orchestration Engine processes order and routes to proper Gateway
- 6) Gateway executes order and sends provisioning commands to respective Data Center or Cloud Resource
- 7) Resource provisions service and sends notification to Gateway
- 8) Gateway via Orchestration Engine updates user account within Storefront
- 9) User and admins have access to resources via Gateway or directly

4.2 Use Case Two

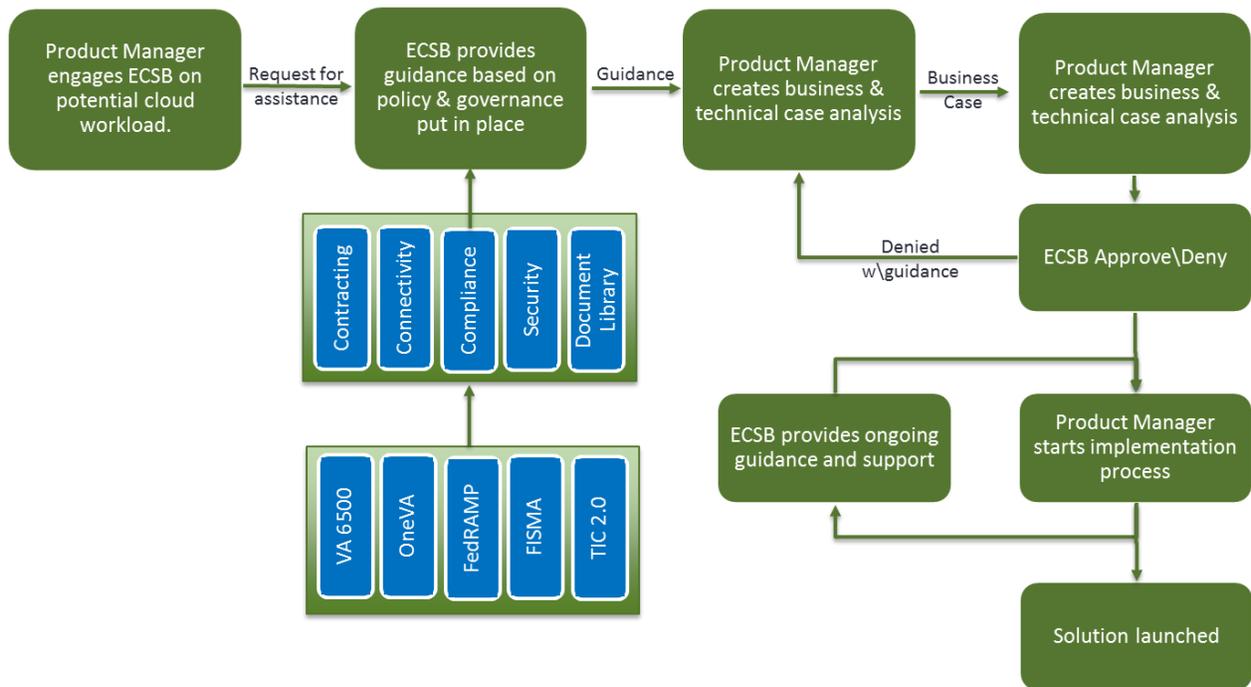


Figure 9 - Business Use Case (Provided by industry partners)

- 1) Product Owner engages ECSB on potential cloud workload
- 2) ECSB provides guidance based on policy and governance
- 3) Product Owner creates business and technical case analysis
- 4) ECSB approve/deny
- 5) ECSB provides ongoing guidance and support
- 6) Product Owner starts implementation process
- 7) Solution launched

Appendix A. DOCUMENT SCOPE

A.1 Scope

This Enterprise Design Pattern focuses on the ECSB required to provide a cloud-based hosting environment for applications. It will define the ECSB program for LOBs to leverage cloud services and outlines the standards and capabilities for an ECSB to act as a liaison between VA (Cloud Consumer) and Cloud Providers. This Enterprise Design Pattern will adhere to VA and federal policies.

This Enterprise Design Pattern will:

- Outline current cloud initiatives within VA and associated challenges
- Define VA's ECSB Program addressing Service Aggregation, Arbitrage, and Intermediation
- Build an overarching use case demonstrating the use, performance, and delivery of cloud services leveraging the ECSB concept

This Enterprise Design Pattern does not:

- Recommend specific tools and technologies
- Define Implementation policy or directive
- Define Cloud Security and Privacy Policies
- Provide project-specific solution architectures

A.2 Document Development and Maintenance

This document was developed collaboratively with internal stakeholders from across the Department and included participation from VA's OI&T, Product Development (PD), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE) and industry. This document contains a revision history and revision approval logs to track all changes. Updates will be coordinated with the Government lead for this document, which will also facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

Appendix B. DEFINITIONS

Key Term	Definition
Cloud Consumer	A person or organization that maintains a business relationship with and uses services from a cloud provider
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties

Key Term	Definition
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.

Appendix C. ACRONYMS

The following table provides a list of acronyms that are applicable to and used within this document.

Acronym	Description
AA&A	Authentication, Authorization and Audit
AITC	Austin Information Technology Center
API	Application Programming Interface
ASD	Architecture, Strategy and Design
ATO	Authority to Operate
CIA	Confidential, Integrity and Availability
COTS	Commercial Off the Shelf
CRM	Customer Relationship Management
CSP	Cloud Service Provider
DHS	Department of Homeland Security
DOD	Department of Defense
EA	Enterprise Architecture
ECSB	Enterprise Cloud Services Broker
EDE	Enterprise Development Environment
ESCCB	Enterprise Security Change Control Board
ETA	Enterprise Technical Architecture
ETSP	Enterprise Technology Strategic Plan
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GFE	Government Furnished Equipment
IaaS	Infrastructure-as-a-Service

Acronym	Description
IAM	Identity and Access Management
IPT	Integrated Project Team
IT	Information Technology
JAB	Joint Authorization Board
LOB	Line of Business
NCA	National Cemetery Administration
NIST	National Institute of Standards and Technology
NSOC	Network Security Operations Center
OI&T	Office of Information and Technology
PATO	Provision Authority to Operate
PHI	Protected Health Information
PII	Personally Identifiable Information
PTA	Privacy Threshold Analysis
SDE	Service Delivery and Engineering
SDLC	Software Development Lifecycle
SLA	Service Level Agreement
SOA	Service-Oriented Architecture
SPI	Sensitive Personal Information
TDEA	Triple Data Encryption Algorithm
TIC	Trusted Internet Connection
TRM	Technical Reference Model
VBA	Veteran Benefits Association
VHA	Veteran Health Administration
VOA	Virtual Office of Acquisition
VRM	Veterans Relationship Management

Appendix D. REFERENCES, STANDARDS, AND POLICIES

This Enterprise Design Pattern aligns to the following VA OI&T references and standards applicable to all new applications being developed in the VA, as well as to the VA ETA:

#	Issuing Agency	Applicable Reference/Standard	Purpose
1	VA OIS	VA 6500 Handbook	Directive from the OI&T OIS for establishment of an information security program in the VA, which applies to all applications that leverage ESS.
2	VA	VA Lockdown	VA Strategy for Adoption of Cloud Computing (draft)
4	VA IAM VA	VA Directive 6051 VA Handbook 6517	Department of Veterans Affairs Enterprise Architecture (VA EA), July 12, 2002 Risk Management Framework for Cloud Computing Services (draft)
5	NIST	NIST SP 500-291 NIST SP 500 -292	NIST Cloud Computing Standards Roadmap, Version 2, July 2013 NIST Cloud Computing Reference Architecture
6	NIST	NIST SP 800 - 145	The NIST Definition of Cloud Computing, NIST SP 800-145, Sept. 2011
7	NIST	NIST SP 500 - 299	NIST Cloud Computing Security Reference Architecture
8	DOD	DOD	Department of Defense cloud computing strategy
9	GSA	GAO 14-753	These challenges were derived from DoD Cloud Computing Strategy and the GAO Report 14-753, "Cloud Computing: Additional Opportunities and Savings Need to Be Pursued," Sept. 2014

#	Issuing Agency	Applicable Reference/Standard	Purpose
10	OMB	OMB M-08-05, Implementation of Trusted Internet Connections (TIC)	<p>Establishes TIC to optimize and standardize the security of external network connections for Federal agencies. Three strategic components:</p> <ul style="list-style-type: none"> • Reduce and consolidate external access points • Manage security requirements for NOC/SOC • Establish compliance program to monitor adherence to TIC policy
11	Federal	U.S. CIO, Federal Cloud Computing Strategy	This policy is intended to accelerate the pace at which the Government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments.
12	Federal	U.S. CIO, 25 Point Implementation Plan to Reform Federal Information Technology Management	States that the Federal Government will shift to a “Cloud First” policy to better prepare the Government for future computing needs. When evaluating options for new IT deployments, OMB will require agencies to default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists.
13	Federal	FIPS 199 FIPS 200	<p>FIPS 199 (Federal Information Processing Standard Publication 199)</p> <p>Minimum Security Requirements for Federal Information and Information Systems</p>
14	VA	VA Memorandum Consideration of Open Source Software (VAIQ#7532631)	Establishes requirements to evaluate Open Source Software solutions and consider OSS development practices for VA-developed software.