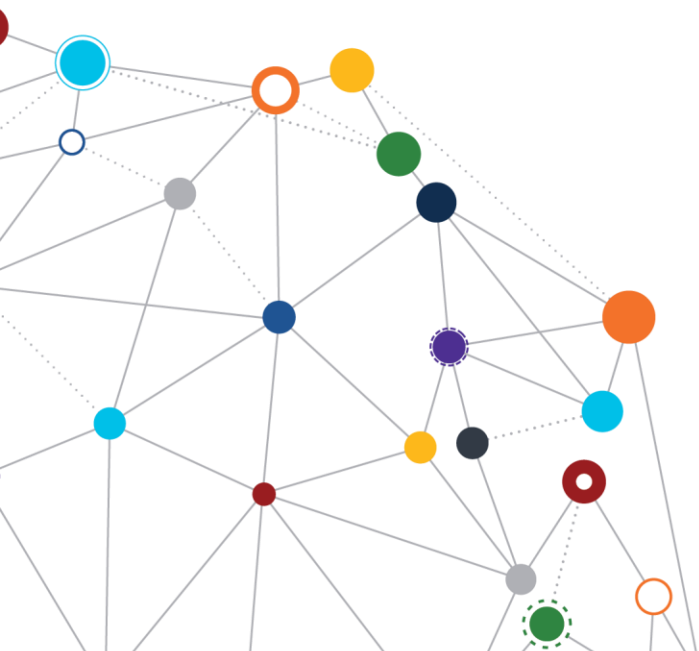OFFICE OF
INFORMATION
AND TECHNOLOGY

Cloud Computing at the Department of Veterans Affairs

White Paper

August 2018| OIT, EPMO, Demand Management Division

Table of Contents

1   Introduction

The Department of Veterans Affairs (VA) has taken significant steps toward advancing effective collaboration among workstreams by strengthening the relevance of cloud computing through enterprise-wide strategy, planning, and decision-making. In the VA Fiscal Year (FY) 2018-2024 Strategic Plan,[1] the need to modernize systems and technology is described among the five priorities to enable Veterans and VA employees "to deliver the high-quality care and services Veterans deserve."[2] Concurrently, the VA information technology (IT) Modernization Guiding

> *The implementation of cloud agility, scalability, maintainability, and cost predictability is a VA IT Modernization Guiding Principle.*

Principles include the implementation of cloud agility, scalability, maintainability, and cost predictability. The evolution of cloud adoption at VA promises to promote agile product delivery, data sharing, enhanced security, stewardship of resources, and customer empowerment.

The VA Office of Information and Technology (OIT), Enterprise Program Management Office (EPMO), Demand Management Division's (DMD) Office of Architecture and Engineering Service (AES) works with the Enterprise Cloud Solutions Office (ECSO) to provide high-level technical direction for using the VA Enterprise Cloud (VAEC). This white paper addresses real-world examples of the benefits and constraints of cloud implementation; thought leadership on cloud computing at VA; and plans to enhance customer service and improve product satisfaction for the benefit of our Nation's Veterans.

2   Overview of Cloud Computing

Cloud computing is defined by the National Institute of Standards and Technology (NIST) as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.[3] Cloud computing adoption is a business decision. In addition to enabling agile product delivery, data sharing, and enhanced security, cloud adoption reduces the IT burden for both developers and operations staff.

The cloud network of remote resources is hosted on the Internet to store, manage, and process data, rather than on a local server or a personal computer. The remote resources include virtual servers, storage, secure network connections, and services. These cloud services use models that are defined by NIST as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS).

---

[1] https://www.va.gov/oei/docs/VA2018-2024strategicPlan.pdf
[2] https://www.va.gov/oei/docs/VA2018-2024strategicPlan.pdf
[3] https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published

There are five key components that highlight cloud computing at VA. These components are based on NIST recommendations for architecture framework, enabling VA to maximize the benefits of migrating to cloud services.

1) **Cloud Consumer** – A person, or organization that maintains a business relationship with, and uses service from Cloud Providers.
2) **Cloud Auditor** – A party that can conduct independent assessment of cloud services.
3) **Cloud Provider** – A person, organization, or entity responsible for making a service available to Cloud Consumers.
4) **Cloud Broker** – An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.
5) **Cloud Carrier** – The intermediary that provides connectivity and transport of cloud service from Cloud Providers to Cloud Consumers.

While the NIST cloud model is comprised of five service characteristics, three service models, and four deployment models, OIT has transitioned away from the role of cloud broker.

2.1   Cloud Service Essentials

VA is adopting an enterprise cloud strategy to be more responsive to its VA customers. The VAEC provides five service essential characteristics that make developing, supporting, and maintaining applications easier.

1. **On-demand self-service** – A VA accredited cloud service is orderable, configurable, and manageable by way of a self-service service portal web/mobile interface. Control to this interface is fully manageable (role-based) and enforced upon each request.
2. **Broad network access** – No special networks are required; services are available through standard access mechanisms and standard VA devices.
3. **Resource pooling** – A central cloud orchestration engine manages "pools" of commodity based resources and exposes them to customers as a service.
4. **Rapid elasticity** – Organizations can use what is currently needed and scale as the load and use demands increase. High utilization is the goal (60-80 percent).
5. **Measured service** – Elasticity, pooling, and capacity management depend on accurate, actionable measures. Every aspect of the service must be measurable: access, performance usage, cost, etc.

2.2   Service Models

The business requirements define the "As a Service" component to the cloud with infrastructure, platform, and software. These high-level service models host and manage underlying services that are based on the shared responsibility model. This model recognizes that both the developers using the cloud, and the cloud providers, each have responsibilities for delivering secure IT services to customers. The level of customer management helps to define the service model; it is infrastructure, when the customer provides the platform and software; it is platform, when the customer provides the software; or it is software, when the customer

provides the designs, configurations, and code that needs to be hosted and manages the application changes.

- **IaaS** – The customer can provision fundamental computing resources, while the vendor manages the underlying cloud infrastructure, which is the collection of hardware and software that enables the cloud services being provided to the cloud customer.
- **PaaS** – The customer can deploy consumer-created or acquired applications that are created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure.
- **SaaS** – The customer can use the provider's applications as it runs on a cloud infrastructure. Examples include web-based email services and SaaS productivity software, such as the customer relation management (CRM) software, Salesforce, and the suite of office productivity software, Microsoft Office 365.

The VAEC implementation of the service models is to leverage economies of scale and the use of shared services. The VAEC primarily implements the IaaS and PaaS models; most SaaS applications run in a vendor's cloud. The analysis and planning of each application will help to determine the specific service model to implement on a case-by-case basis.

2.3 Deployment Models

Cloud deployment models are often categorized on the basis of access and proprietorship, and include security and cost as factors that help to determine the appropriate deployment model. Cloud deployment methods also coincide with the business requirements of the cloud service models; IaaS, PaaS, and SaaS have their own versions of provisioning and deployment.

- **Private Cloud** – All resources are dedicated to a single organization. Resources are owned, managed, and operated by the organization or managed service provider. A private cloud provides a maximum level of security. It is the best choice for organizations that need to manage their host and customer applications.
- **Community Cloud** – Like a public cloud, all resources are shared, but they are only accessible to a target community of users.
- **Public Cloud** – The public cloud infrastructure will be in the premises of the service provider, but it is entirely shared and operated by the organizations using it. It may have the ability to provision dedicated resources, but it is part of an entirely shared ecosystem, and it is generally available to the public. Even though all resources are shared, the data is kept private, with reasonable levels of security and low operational costs.

- **Hybrid Cloud** – As its name implies, it is a combination of any of the other cloud models. Typically, it is a mix of private and public/community clouds, where sensitive workloads are kept in the private cloud, and other workloads operate in the shared cloud models. Operational costs will reflect the need to manage diverse environments to ensure reliability.

3   Cloud Computing in Industry

In addition to reducing the need to fund hardware and software, cloud computing also reduces opportunity costs. Cloud computing offers prospects for new modernization that has resulted in disruption of entire industries.

According to a study by Forbes, **cloud computing market revenue is projected to increase to $162 billion in 2020, from $67 billion in 2015.** A report from *The Economist Intelligence Unit* and International Business Machines (IBM) indicated that among 572 business leaders surveyed, approximately three-fourths indicated that their organizations piloted, adopted, or heavily implemented cloud in their organizations.

The cloud also provides cloud cost flexibility when online marketplaces gain access to more powerful analytics online. For example, Etsy, an online organization that markets handmade goods, used cloud-based capabilities to analyze data from approximately one billion monthly views of its website; Etsy used the information to create product recommendations.[4] The cost flexibility from cloud offered Etsy the use of tools and computing power that might have only been affordable to larger retailers in the recent past.

> *According to a study by Forbes, cloud computing is projected to increase to $162B in 2020, from $67B in 2015.*

Many executives believe that cloud computing can help them adapt to unique user groups, with a diverse combination of devices.

Cloud computing also offers scalable usage through subscription models. In other words, the customer only pays for the computing resources they need. The resources are important in managing spikes in demand, without the need to permanently invest in computer hardware. Netflix, for example, leverages this benefit to its advantage. Due to its on-demand streaming service, Netflix faces large surges in server load at peak times. The move to migrate from traditional data centers to public cloud service providers has significantly expanded the company's customer base, without having to invest in the setup and maintenance of costly infrastructure.

4   Usage at VA

---

[4] https://www.fastcompany.com/40567081/why-etsy-is-moving-its-data-centers-to-the-cloud

The VAEC is supported by the ECSO to implement the VA Cloud-First Policy that is articulated in VA Directive 6517, *Cloud Computing Services.*[5] The ECSO will guide VA leaders and project teams to identify opportunities to align cloud-related project activities. In doing so, the ECSO is expected to provide a platform that follows standard processes and procedures that all IT projects can use to deliver products, using new methodologies and approaches, such as agile and development operations (DevOps).

The VAEC is also advanced by the joint Strategic Sourcing and DMD's *Use of the VAEC to Host Applications* Memorandum.[6] The VAEC is intended to be VA's main destination for building new cloud applications and for migrating existing applications to the cloud. Today, the VAEC consists of two cloud service providers: [Microsoft Azure Government](#) and [Amazon Web Services (AWS) GovCloud](#). The VAEC will expand to include an on-premise VA Private Cloud by the end of FY19.

From the VA Cloud Strategy draft, the VA Chief Information Officer (CIO) will initiate a three-phase IT strategy to adopt and optimize cloud computing. The IT strategy enables VA to adapt its organization, policy, processes, and culture to achieve VA mission goals and overall business priorities. This process includes laying the foundation to enable the start of new cloud-native services and applications. The foundation enables agile delivery and consumption of digital services that enhance the customer experience; and it supports the VA IT Modernization Guiding Principles[7] that are related to the migration of legacy systems to a modern IT infrastructure.

The VAEC is designed to streamline the workflow for project teams by representing a common, logical platform architecture that is based on open standards. In addition, application programming interfaces (APIs) and standard onboarding processes simplify access to shared services for new application development or modernization of legacy systems. For example, the General Support Services (GSS) toolkit is a collection of cloud-based services that help project teams connect existing systems to the VAEC, or create new systems that run in the VAEC natively. This results in faster time-to-market for new Veteran-facing services and greater flexibility as the business needs and strategic priorities change. The VAEC was officially launched in September 2016, and approximately 25 applications have begun using the VAEC as of March 2018. Current VAEC applications in production include *Caseflow Appeals*, *Digital Veterans/API Platform* (formerly *Lighthouse*), *Online Patient Self-Scheduling System* (*FasterCare*), and *Vets.gov*.

- [Caseflow Appeals](#) – Created by the VA Digital Service, this tool helps accelerate the appeals review for benefit claims.
- [Digital Veterans/API Platform](#) – The API management platform provides OIT and external developers with secure access to Veteran data and tools.

---

[5] VA Directive 6517, *Cloud Computing Services;* http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=852&FType=2
[6]
https://vaww.portal.va.gov/sites/ECS/_layouts/15/WopiFrame2.aspx?sourcedoc=/sites/ECS/Shared%20Documents/Cloud%20101/FY18%20Cloud%20Policy%20180116.docx&action=default&DefaultItemOpen=1
[7] OIT 2017 Year in Review;
https://www.oit.va.gov/library/reports/yir_2017.pdf?utm_source=homepage&utm_medium=link&utm_campaign=year-in-review; Accessed on 12 June 2018

- FasterCare – VA responded to the Faster Care for Veterans Act of 2016 by launching a program that allows Veterans to schedule, cancel, and reschedule VA appointments ubiquitously; anytime, anywhere, and from any device. In addition, VEText, a text messaging appointment-reminder system, reminds Veterans of upcoming appointments, and allows them to confirm or cancel appointments. Since the time of the VEText deployment at 138 VA facilities last March, no-show medical visits have been reduced by more than 100,000.
- Vets.gov – The website enables Veterans to discover, apply for, track, and manage the benefits they have earned. It provides a common platform for Veteran-facing services that combine multiple sites that are supported by individual business lines.

The VAEC has been defined in VA's Enterprise Architecture (EA) through the adoption of enterprise standards and VA Guiding Principles.

Enterprise Design Patterns (EDPs) that relate to cloud computing have been available to project managers since 2015 to help establish common terminology, standards, and capabilities that are needed to support VA's digital transformation. Additionally, the ECSO has been established to implement the VAEC and other cloud solutions that deliver secure and seamless cloud functionality to support the entire VA enterprise. ECSO enables internal and external VA stakeholders to leverage cloud solutions by providing standardization and common services. ECSO supports efficient migration and utilization of cloud technology by project teams, business sponsors, and their customers.

A recommended 10-step process is under development and will make the migration to cloud repeatable and manageable. The 10-step process for the end-to-end Application VAEC Cloud Implementation is listed in Table 1.

Table 1: 10-Step Process for End-to-End Application VAEC Cloud Implementation

Step	Description
1. **VAEC Request Submission**	The initial VAEC engagement in tandem with Veteran-focused Integration Process (VIP) request to coordinate service agreements and funding needs to support discovery. Close attention to Authority to Operate (ATO) preparation with VIP, Information Security Officer (ISO) assignment, and Enterprise Security Change Control Board (ESCCB) process alignment.
1a. Candidate request proposed and pre-processed via VIP Initiation – VIP[3]	The ECSO uses a Cloud Service Provider (CSP) resource Checklist for Technical Reference Model (TRM), ATO, Privacy Information Assessment (PIA), VIP Project, funding documentation etc. Use of VAEC intake notifications to leverage ECSO resources for consulting on cost budget data and support data for cloud decisions.

2.	VAEC Pre-Intake	The initial engagement with VAEC as part of a VIP project initiation requesting cloud implementation. The candidate application must have completed the VIP Request (VIPR) initiation process and as such must have derived the cost estimates using these sources: Budget Tracking Tool (BTT)/Primavera historical product cost data/Integrated Funds Control, Accounting, and Procurement (IFCAP), and others, and must be documented/Capital costs, as part of Development, Maintenance, and Enhancement (DME) any additional Software and licensing. The VAEC team has documented the cost estimation tools and the licensing options for common software (SW): RedHat, Windows, SharePoint, Structured Query Language (SQL), etc. via VA Enterprise Agreements or Pay-As-You-Go (PAYG) options.
3.	ECSO VAEC Intake	The engagement of ECSO Cloud resources: The Critical Decision 1 (CD1) is ascertaining if the candidate meets the cloud criteria. Once CD1 is approved within VIP, the next step is assessment of CSP environment and the Enterprise Service Cloud Request (ESCR) Form is required along with Requirements Checklist.
4.	ECSO VAEC Initial Estimations application provision preparation analysis	The cloud requirements refined and documented, Application Team Project Manager (PM) Updates Rough Order of Magnitudes (ROMs), Acquisition Review Module (ARM), formerly IT Acquisition Request System (ITARS) site - http://vaww.va.gov/itt/, 2237 processed (pre-requisite for provisioning).
5.	ECSO VAEC Application assessment svc model selection	At this point, the application team is compliant with technical and funding requirements for initial cloud provisioning. This includes the Enterprise Cloud Funding Agreement Form with the Strategic Programming Item (SPI) Strip detail and amount provided by application owner as part of the VIP process.
6.	VAEC Setup	Complete the provisioning Guide to pre-load the CSP Cloud setup and provisioning with Operations. The Critical Decision 2 (CD2) is having funding and acquisition orders approved.
7.	VAEC Provisioning	The VAEC team takes the outcomes of the analysis and together with the Information Technology Operations and Services (ITOPs) and CSP teams fills in the details for scripts, automation runbooks, and operation handoff. Each application owner team must attain their respective application ATO building on the existing ATOs for the core services of each approved CSP (AWS/Azure). The outcomes include the details for cloud constructs such as virtual machine (VM) counts/types, subnets/Internet Protocol (IP) Addresses, data bandwidth considerations, database sets, etc.
8.	VAEC Application Hand-Off to Operations – the point at which cloud environment is ready for usage	In the VAEC, we leverage CSP Intrinsic Accounts to enable the management and creation of the underpinning infrastructure among core VAEC Team members. As well as application team accounts to enable the administrator roles within the team to create and manage the allowed resources for their corresponding environment (VMs, storage, network configurations, accounts/groups, etc.) on top of the underpinning infrastructure already in place. The Operations handoff validation of roles responsibilities, Service Level Agreements (SLAs), and business continuity (failover, fail back, back up, etc.).
9.	ECSO VAEC Application Operations Lifecycle	The transition point from provision to operations uses checklist and an Operations Readiness Review.
10.	ECSO VAEC Application Decommission	Decommissioning still follows a VIP process, but is in a reverse order of the implementation and migration

5 Thought Leadership

Historically, VA attacked problems in silos, where any given IT project team was responsible for solving all its own hosting requirements, building its own code, and deploying its application using any approach. The new focus is to provide a standardized cloud environment of shared services and applications, providing common security, and speeding up application deployment, without duplication.

Mr. David Catanoso, Director of ECSO, states that the transition into the VAEC will create a positive impact on the security and business architecture, and the ability to leverage shared services. Using established cloud governance processes, the VAEC can be expected to simplify the creation of applications, while creating greater security with a smaller infrastructure footprint. The VAEC will impact business processes related to managing IT resources and help answer questions such as the following:

- How will moving to the cloud improve business operations, rather than using a typical data center?
- From an operational perspective, what are the benefits of the cloud?
- From the business owner's perspective, what is required to move to the cloud?
- What is the cloud doing differently from what we are currently doing?

The information contained in the cloud needs to be aligned to the VA EA business architecture to show how the cloud operationally aligns to VA business needs.

The VA Systems Inventory (VASI) is an inventory of the main IT systems that support key mission and business functions for VA. Each system has technical information to help support analysis about the types of systems used in VA, and the types of systems needed in VA to support changing business needs. There is some uncertainty if cloud will represent a major shift for VASI. The cloud is essentially another mechanism for providing hosting services for most VASI systems. Once SaaS is leveraged more broadly across OIT, this may change. VASI will certainly be a factor in the overall strategy, including the way product lines are formed, the way systems are reviewed, and the mechanisms for analyzing or reducing the system environment. The expectation is to find cloud implementation standards in an EDP to communicate guidance for system owners across VA. The goal is to see a step-by-step process on how to use cloud, and learn about what standard services are available, and how to configure them.

The key IT systems have hosting environments in VA, and traditionally they have been in VA's data centers, or in offsite environments. With the move to the cloud, most of these systems will be migrated to the VAEC, while some capabilities will remain in VA's data centers on a case-by-case basis.

6   Benefits

The benefits[8] of an enterprise cloud infrastructure include improving VA's ability to target its efforts toward key mission areas that are focused on Veterans. The platforms and software

---

[8] https://www.oit.va.gov/library/programs/ts/edp/cloud/TransitiontoCloud_V1.pdf

services are categorized by costs and shared across a wide customer base and supported by leading, external technology providers. As a result, this will lead to more effective and responsible control of taxpayer dollars. The adoption of the cloud and its benefits to implement new and existing applications will reduce complexity, costs, and aid data center consolidation, while enabling the adoption of the latest technologies to improve services to Veterans. The cloud migration is a many-to-one transformation, where numerous applications hosted across many physical data centers can be hosted within a singular Government Cloud.

The benefits of deploying and migrating to cloud services through the VAEC include the following:

- **Optimize infrastructure and resources:** Reduce data center infrastructure expenditures through simplification, transitioning from fragmented and duplicative systems.
- **Compute on-demand**: Facilitate utility computing, paying only for the virtual resources consumed.
- **Improve uptime**: Use built-in availability that is managed by the service provider.
- Adapt: Elastic computing enables dynamic adaptation of capacity to meet a varying workload.
- **Focus**: Shift focus from managing IT infrastructure to developing business logic.
- **Regularly update**: CSPs regularly update offerings to give the cloud consumer the most up-to-date technology.
- **Reduce risk**: Consistently implement security standards to decrease the risk of insider threat and outside intrusion.
- **Maintain business continuity**: Provide a low-cost option for disaster recovery, replication, failover, and backup storage.
- **Access**: Provide seamless accessibility to cloud-based applications and data from virtually any internet connected device.
- **Collaborate**: Worldwide access means teams can collaborate from a wide variety of locations.
- **Support DevOps processes**: Cloud environments strongly support continuous integration, testing, deployment, and infrastructure-as-code, all key principles under the umbrella of DevOps. Cloud environments act as accelerants in deploying systems to meet requirements.

Moving to the cloud will decrease support costs of legacy systems by shifting from a capital-intensive operating model, freeing up investment dollars to develop more IT-driven Veteran services. Additionally, the cloud will increase efficiency and leverage external vendors with much greater economies of scale, and reduce duplication and licensing fees. When it comes to energy costs, cloud computing uses less electricity, since effectual hardware utilization equates to more efficient use of power at VA.

7   Challenges

The cloud provides flexibility, but an understanding of the current IT environment at VA is required to understand the tradeoffs needed to benefit from migrating to the cloud. One

potential challenge is the limited oversight of systems moving to the cloud, which results in a high total cost of ownership (TCO) for operational support and maintenance of production systems. The VAEC has control systems in place to avoid unexpected costs.

Another challenge is scaling up the capability to move a greater number of applications. To address these challenges, VA is currently adopting IT governance processes and enterprise architecture models to integrate with cloud solution architecture guidelines and project team guidance. The Enterprise Program Management Office (EPMO) is currently evolving the system development lifecycle (SDLC) processes, design guidance, and requirements to streamline the pathways to production for products that are subject to VIP.

8 Future state

The VAEC is operational with significant resources to enable VA to migrate applications. The plan is to migrate over 350 applications in the VAEC by 2024. The number of applications in the cloud is expected to grow exponentially over the next five to seven years, as VA and the ECSO increase capacity to migrate existing applications and build new cloud-based applications. Through the Cloud Strategy and Roadmap, more VAEC functionality is forthcoming, as additional industry agreements and governance processes are implemented.

Additionally, VA intends to provide a private cloud offering to support products that are better suited for the on-premises environments, such as those that store or disseminate protected health information (PHI). VA is migrating numerous enterprise applications, from customer relationship management (CRM) to SaaS products (e.g., Salesforce). VA is also working with the Department of Defense (DoD) to migrate healthcare applications to a DoD-hosted cloud environment; the DoD Cloud acts separately from the VAEC to support electronic health record modernization (EHRM).

Appendix A. Acronyms

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

Acronym	Description
AES	Architecture and Engineering Service
APIs	Application Programming Interfaces
ARM	Acquisition Review Module
ATO	Authority to Operate
BTT	Budget Tracking Tool
CD1	Critical Decision 1
CD2	Critical Decision 2
CIO	Chief Information Officer
CRM	Customer Relationship Management
CSP	Cloud Service Provider
DevOps	Development Operations
DMD	Demand Management Division
DME	Development, Maintenance, and Enhancement
DoD	Department of Defense
EA	Enterprise Architecture
ECSO	Enterprise Cloud Solutions Office
EDPs	Enterprise Design Patterns
EHRM	Electronic Health Record Modernization
EPMO	Enterprise Program Management Office
ESCCB	Enterprise Security Change Control Board
ESCR	Enterprise Service Cloud Request
FY	Fiscal Year
GSS	General Support Services
IaaS	Infrastructure-as-a-Service
IBM	International Business Machines
IFCAP	Integrated Funds Control, Accounting, and Procurement
IP	Internet Protocol
ISO	Information Security Officer
IT	Information Technology
ITARS	IT Acquisition Request System
ITOPS	Information Technology Operations and Services
NIST	National Institute of Standards and Technology
OIT	Office of Information and Technology
PaaS	Platform-as-a-Service

Acronym	Description
PAYG	Pay-As-You-Go
PHI	Protected Health Information
PIA	Privacy Information Assessment
ROMs	Rough Order of Magnitudes
SaaS	Software-as-a-Service
SDLC	System Development Lifecycle
SLAs	Service Level Agreements
SPI	Strategic Programming Item
SQL	Structured Query Language
SW	Software
TRM	Technical Reference Model
USDA	United States Department of Agriculture
VA	Department of Veterans Affairs
VAEC	VA Enterprise Cloud
VASI	VA Systems Inventory
VIP	Veteran-focused Integration Process
VIPR	VIP Request
VM	Virtual Machine