VA Enterprise Design Patterns
Privacy and Security

Cloud Security

OFFICE OF TECHNOLOGY STRATEGIES (TS)
OFFICE OF INFORMATION AND TECHNOLOGY (OI&T)

VERSION 1.0
DATE ISSUED: SEPTEMBER 2016

APPROVAL COORDINATION

Gary E. Marshall 137891

Digitally signed by Gary E. Marshall 137891
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=gary.marshall@va.gov, cn=Gary E. Marshall 137891

Date: 2016.09.15 07:31:25 -04'00'

Gary Marshall
Director, Technology Strategies, ASD

PAUL A. TIBBITS 116858

Digitally signed by PAUL A. TIBBITS 116858
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=paul.tibbits@va.gov, cn=PAUL A. TIBBITS 116858
Reason: I am approving this document.
Date: 2016.09.28 10:35:40 -04'00'

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

REVISION HISTORY

Version	Date	Approver	Notes
1.0	7/1/2016	Nicholas Bogden	Updated draft incorporating stakeholder inputs, community review, and drafted based on comments received prior to TS leadership approval.

CONTENTS

1 Introduction 5
1.1 Business Problem 5
1.2 Business Need 6
1.3 Business Case 6
1.4 Approach 7
2 Current Capabilities and Limitations 7
2.1 Lack of Defined Policy for Cloud Deployments 8
2.2 Confusion Over TIC Compliance Requirements 8
2.3 Restricted Use of Cloud Computing Resources Due to Security Risks 8
2.4 Lack of Centralized Risk Management for Cloud 9
3 Future Capabilities 9
3.1 Trusted Internet Connection (TIC) Compliance 10
3.2 FEDRAMP Primer 13
3.3 Cloud Encryption 15
3.4 Auditing of Cloud Services 16
3.5 Cloud Availability 17
3.6 Alignment to the One-VA Technical Reference Model (TRM) 18
3.7 Alignment to Veteran-Centric Integration Process (VIP) 18
4 Use Cases 19
4.1 Healthcare Application on a Private Cloud 19
4.1.1 Purpose 19
4.1.2 Assumptions 19
4.1.3 Use Case Description 19
4.2 VA Website Hosting General Information on a Medical Condition 20
4.2.1 Purpose 20
4.2.2 Assumptions 20
4.2.3 Use Case Description 20
4.3 Information Sharing Website and Blog Migration to the Cloud 20
4.3.1 Purpose 20
4.3.2 Assumptions 21
4.3.3 Use Case Description 21
Appendix A. Scope 22
Appendix B. Definitions 23
Appendix C. Acronyms 26
Appendix D. References, Standards, and Policies 28
Appendix E. Cloud Security Sample Architecture 30

Table 1: Business Benefits 7
Table 2: Mapping of Future Capabilities of Business Problems 9
Table 3: Shared Responsibility Model 14
Table 4: List of Approved Tools and Standards for Cloud Security 18

Figure 1: Agency Restricted Access Data 12
Figure 2: CSP Data Path Requirements 12
Figure 3: Sample Cloud Security Architecture Overview 30
Figure 4: Cloud Security Sample Architecture VPC Highlights 31

QUICK JUMP

Select an icon to skip to a section.

Current Capabilities

Future Capabilities

Use Cases

One-VA Technical Reference Model

The Veteran-Focused Integration Process

Enterprise Design Pattern Scope

1 INTRODUCTION

The Department of Veterans Affairs (VA) adopted a "Cloud First" policy in response to the Federal Cloud Computing Strategy issued by OMB in 2011. VA already has 12 systems in private clouds and 11 systems pending deployment to public clouds designed for customers that are required to comply with federal requirements. These requirements include the Federal Risk and Authorization Management Program (FedRAMP), Trusted Internet Connection (TIC) Reference Architecture 2.0, and Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG). Despite the growing number of cloud deployments both across the federal sector and within VA, cloud security remains a primary concern for customers considering cloud adoption due to the need to trust the Cloud Service Providers (CSP) in areas where the customer cedes control.

1.1 Business Problem

VA is still in the process of establishing an Enterprise Cloud Service Broker (ECSB) and policies related to required security controls to ensure consistent and secure use of the cloud. FedRAMP published Low and Moderate impact baselines for use by CSP and federal agencies. This helped to guide the migration of lower risk applications to the cloud; however FedRAMP had not published a High impact baseline which would apply to FISMA High rated systems until recently, on June 23, 2016. This left a gap in guidance on risk management for moving the most sensitive VA information into the cloud which applies to several core VA services. FedRAMP requires TIC compliance for cloud, but VA will educate stakeholders on how to consistently accomplish this. Routing cloud traffic through the VA TIC can introduce latency and excess

bandwidth costs without providing full traffic inspection which must be considered. VA needs guidance on how cloud security is different from traditional, on premise security. Current challenges to cloud deployments include:

- Lack of defined policy for cloud deployments
- Confusion over TIC compliance requirements
- Restricted use of cloud computing resources due to security risks
- Lack of centralized risk management for the cloud

1.2 Business Need

VA mandates using cloud first. A number of projects are lined up for migration to the cloud. Existing cloud projects may be at risk due to architecture designs, hosting FISMA High systems within a boundary that do not meet FedRAMP High or CSP instability. While the ECSB is being established and policy created, VA stakeholders need guidance now to minimize risk.

- Establishing cloud security standards in VA will assist cloud projects in understanding the following:
- Available options for achieving TIC compliance and the impacts on their project What FedRAMP means and how to implement strong controls
- Federal Information Processing Standards (FIPS) compliance as well as how encryption impacts risk
- Auditing challenges and considerations for monitoring cloud projects within VA
- How to select a CSP and cloud architecture that meets the project risk profile for availability

1.3 Business Case

While TIC compliance is currently required, stakeholders may not be familiar with sample architectures available. A lack of TIC compliance has caused past cloud migration projects to fail. Providing one or more recommended options will allow more efficient migrations to the cloud and more effective cost estimating based on resource utilization. Most CSPs tout the ability to more closely monitor activity in the cloud through monitoring of Application Programming Interfaces (API). This only provides a benefit when connected to the appropriate VA service to perform the monitoring and investigate anomalies. Consistent monitoring will reduce the risk of compromise while proper cloud controls are established. Establishing architecture to support risk management and compliance will enable faster cloud adoption, more securely.

Table 1 shows the overall benefits to establishing cloud security standards to support cloud-enabled business needs that will yield improved returns on investment (ROI) and lower total costs of operations (TCO):

TABLE 1: BUSINESS BENEFITS

Business Benefits	Description
Greater Cloud Project Compliance	More clearly defined compliance requirements for cloud projects will help project managers focus more on business requirements while creating compliant solutions from the beginning.
Better Risk Management	Use of the cloud can increase risk due to new exposure, multiple vendors, varying interfaces, and custom tools. Centralized monitoring of cloud projects can create better visibility for tracking data access and making risk-based decisions.
Standardized Controls to Increase Flexibility	A standard template for cloud deployments will allow VA to evaluate more CSPs to determine the best cost solution instead of primarily limiting projects to one private cloud vendor.

1.4 Approach

The following steps define a near-term path toward strengthening the security of messages traveling within the VA network. This is particularly relevant for existing production systems that cannot guarantee end-to-end transport security. In the long run, VA will adopt cloud services that enable end-to-end transport security (both for data at rest and data in transit). Cloud services will include built-in functionality to support message-level security. More information on cloud services and cloud security can be found in the Cloud Computing Architecture and Cloud Security EDPs.

2 CURRENT CAPABILITIES AND LIMITATIONS

VA started moving to the cloud using contracted integrators in 2012. Although VA Directive 6517 established the roles and responsibilities at that time, VA is still working to establish an ECSB to guide stakeholders. In this, VA is limited to a Cloud Integrated Project Team (IPT). VA mainly deploys private cloud solutions using Verizon Terremark and a smaller subset of Software as a Service (SaaS) solutions hosted in private implementations at various vendor facilities. While VA has roughly a dozen projects using a private cloud, it has almost as many projects evaluating community or other types of cloud hosting. Despite this “Cloud First” push,

there are a number of challenges, to increasing flexibility and reducing cost by moving to the cloud. These challenges are detailed in the following sub-sections.

2.1 Lack of Defined Policy for Cloud Deployments

The advent of FedRAMP was meant to make the cloud adoption process easier for federal agencies. FedRAMP provides baseline controls for Low and Moderate risk systems, and is designed to reuse authorization packages to shorten the Authority-To-Operate (ATO) process. It also provides a minimum set of controls and does not account for any controls required by each agency. VA is still required to assess the controls provided by the CSP against their own baseline to issue an ATO. There are several challenges in this area. FedRAMP evaluated a High baseline for over a year, which was recently released in June. VA has not defined a set of agency controls required for cloud projects at each FISMA level yet as the Office of Cyber Security (OCS) continues to develop policy for this area.

2.2 Confusion Over TIC Compliance Requirements

CSPs make a number of claims related to different areas of compliance such as TIC, FIPS, FISMA, and others. Although compliance may be achievable in these areas, the default solution provided by the CSP may not be compliant, and it may not be clear how to achieve compliance. Failing to meet TIC compliance delays some cloud projects in order to redesign for compliance. Others fail after committing resources. The TIC Gateways are managed by the VA-NSOC which is responsible for TIC compliance. VA currently has two architectures which can be used for TIC compliance. Lack of a centralized location for sharing cloud information with stakeholders may delay consideration of TIC compliance until change control board reviews are performed.

2.3 Restricted Use of Cloud Computing Resources Due to Security Risks

Before a FedRAMP High baseline and defined supplemental controls from VA, many projects defaulted to the Private Cloud model using a single vendor. Enterprise Operations deployed its own cloud across two physical sites based on VMware, which is adding features to catch up with major CSPs. There is not yet an efficient path forward for projects to adopt cloud based on their FISMA rating; projects may be restricted in their hosting selections which can increase cost unnecessarily. Some CSPs also claim to be FIPS 140-2 compliant, but do not fully explain that compliance is limited to specific parts of the architecture, leaving the system partially compliant.

2.4 Lack of Centralized Risk Management for Cloud

The primary enterprise protection for cloud projects is currently based on TIC compliance. For projects that are TIC compliant, monitoring is performed by VA-NSOC as network traffic moves through the TIC security stack. Even this is limited as traffic is not decrypted and some protections can be evaded. The rest of the cloud projects are protected by a myriad of differing CSP incident response plans and custom monitoring tools. Although CSPs provide logging of APIs and events, these are not centrally collected and analyzed, as VA lacks an Enterprise Auditing solution to provide this service.

3 FUTURE CAPABILITIES

Cloud security is the primary factor that delays projects across both the federal and commercial sector from adopting cloud. Note that CSPs made significant progress in providing strong security for their infrastructure and this will be further enhanced by FedRAMP High. However, VA is still responsible for any data or software it places in the cloud including mitigating related vulnerabilities. Despite the many fears about cloud, organizations adopting cloud have often reported visibility into cloud operations as a top concern.[1] The cloud poses more complex security challenges in addition to the many included with on premise hosting.

TABLE 2: MAPPING OF FUTURE CAPABILITIES OF BUSINESS PROBLEMS

Business Benefits	Description
TIC Compliance	Ensure cloud projects are TIC compliant, thus decreasing network security risks.
Strong Cloud Controls	Provide guidance for minimizing risk while VA controls are in development.
Protect Sensitive Data	Identify when and how encryption can mitigate cloud risks.
Cloud Visibility	Set expectations for audit logging goals to create cloud visibility.
Cloud Availability	Identify major challenges for consideration to reduce risk related to cloud service availability.

The following section highlights critical areas for review, and provides guidance for deploying compliant, secure cloud solutions. To accompany these descriptions, Appendix E also provides a cloud reference architecture showing the interactions of several security services including the TIC gateway identify and access management, FedRAMP zones, and other key components of a secure cloud solution.

[1] https://www.sans.org/reading-room/whitepapers/analyst/orchestrating-security-cloud-36272

3.1 Trusted Internet Connection (TIC) Compliance

TIC provides a critical layer of protection for cloud controls. Cloud projects without TIC protections in addition to a lack of enterprise event management would create an extremely high risk scenario with limited visibility to manage that risk. Not only is TIC compliance a VA requirement, but it is also a FedRAMP requirement. VA experiences various challenges in creating TIC compliant architectures for cloud. To mitigate these challenges, this document provides requirements for TIC compliance in the cloud, and recommended solutions.

Considerations for TIC Integration

- **FedRAMP Enforcement:** All agencies are required to comply with FedRAMP when procuring and using cloud services. While FedRAMP requires connections to federal cloud resources to first traverse a TIC or Managed Trusted Internet Protocol Service (MTIPS), it leaves enforcement of this requirement to each agency. This increases the importance of a VA ECSB to prevent any cloud project from moving forward without going through a common process to ensure FedRAMP compliance. GAO has already identified projects that have increased risk by not following best practices, such as VA's eKidney project.[2] Restriction at the procurement level is required to ensure cloud projects do not move forward without FedRAMP and VA policy compliance. The ECSB can inhibit circumvention at the procurement level by establishing itself as the VA POC with CSPs as well
- **Routing Latency:** The current requirement is that all traffic traverse the TIC and not connect directly from the internet to federal resources in the cloud. This adds some latency due to the extra hops required. Creating faster connections from the VA gateway to the cloud provider, such as direct connections, may be one method to compensate for this additional overhead
- **Approval Authorities:** Cloud projects flow through the standard change management process. For questions on whether a project is TIC compliant, the VA-NSOC will provide a final determination
- **Restricted Access Data:** Protect all Restricted Access Data behind the TIC Gateways. Only Unrestricted Access Data may be accessed directly from the internet. For those unsure of which data is Restricted and Unrestricted, the basic litmus test is "Can an employee/contractor place the data on www.va.gov without requesting authorization?" If the answer is no, the data has Restricted access. Stakeholders are to assume all data is Restricted Access Data unless certified as Unrestricted. Unrestricted Data and Restricted Data must be segregated in the cloud.

[2] http://www.gao.gov/assets/680/676395.pdf

- **Encryption and the Authorization Boundary:** TIC requires encryption up to the edge of the authorization boundary, not just the CSP network. This can be a problem with some CSPs. Some vendors have solutions for SaaS projects which can encrypt data before it goes to CSP leaving only selected metadata in clear text to support indexing and searching. This may mitigate risk related to boundary issues, but may require a Risk Based Decision (RBD) in these instances
- **TIC Network Traffic Decryption:** VA-NSOC may require network traffic be decrypted for inspection within the TIC security stack. Stakeholders should understand how encryption keys are managed and whether or not decryption is possible when preparing to discuss TIC compliance

Implementation of CSP Data Segmentation

To prevent non-government co-tenants from inclusion in any direct network connections, segment data paths between the CSP and VA's networks. Some segmentation, such as Virtual Private Clouds, are reliant on the CSP to ensure some areas of separation. VA is responsible for reviewing the CSP controls to ensure they are sufficient. According to TIC 2.0 Appendix A, FISMA High systems that are externally hosted require physical segmentation (i.e. airgap) from other clients at the hosting provider. With the publishing of FedRAMP High, FISMA High systems in the cloud follow TIC 2.0 Appendix H which requires logical segmentation for compliance. Below are several graphics that illustrate the TIC requirements in relation to CSP data flows.

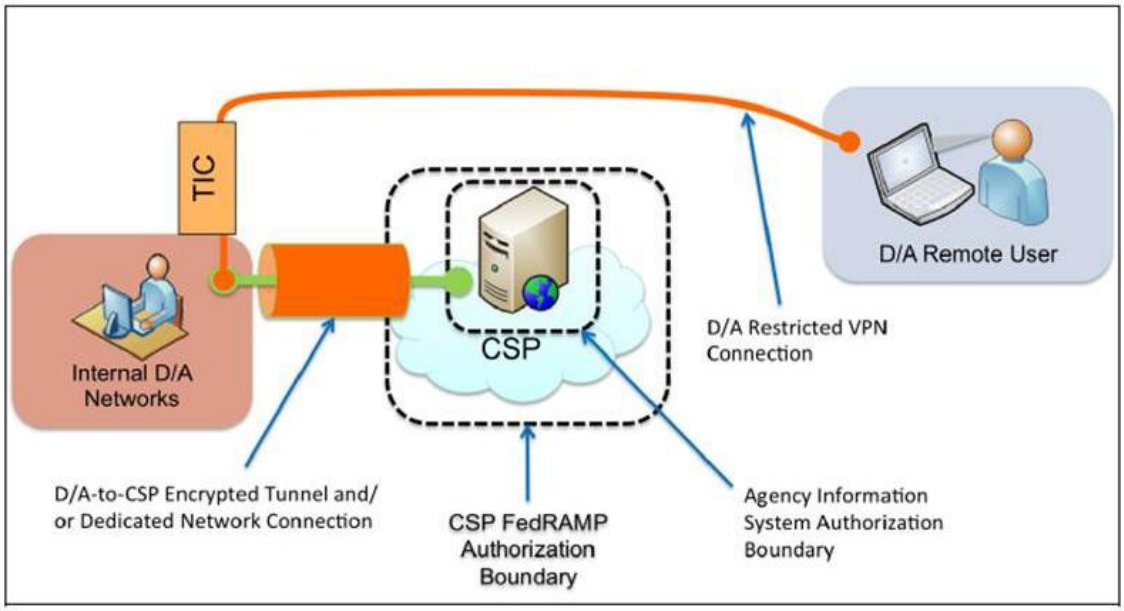

FIGURE 1: AGENCY RESTRICTED ACCESS DATA

In the figure above the remote user connects to the agency VPN before attempting to access the cloud resources. The VPN directs the user through the TIC. Note that the encrypted tunnel between the TIC and the CSP terminates at the Agency Information System Authorization Boundary.

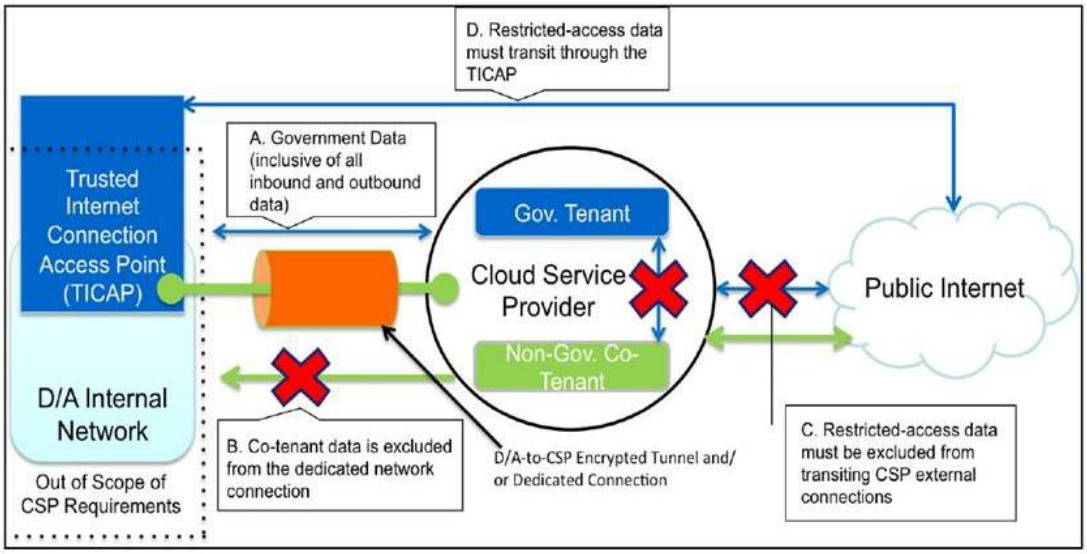

FIGURE 2: CSP DATA PATH REQUIREMENTS

Figure 2 highlights the data path restrictions for CSPs. There are three areas where access is restricted:

- Data does not flow between co-tenants within the CSP
- The data hosted by the CSP cannot be directly accessed from the public internet
- Only the agency's data is traversing the direct connection or VPN between the CSP and the agency

3.2 FEDRAMP Primer

Many stakeholders already have some familiarity with FedRAMP. This section will highlight the security implications of FedRAMP for VA. If you require further detail on FedRAMP, see Appendix D. FedRAMP was designed to improve security consistency through control baselines as well as accelerate adoption by reuse of assessments and authorizations. While the baselines are helping to provide more consistency from the CSPs, there are still some challenges to consider:

- **Not all services will have a FedRAMP ATO** - While some CSPs advertise their FedRAMP ATO, this often does not include all services which are available. A review is still needed to determine which areas have authorization
- **Risk acceptance of the CSP role** – There are some controls for which the CSP is solely responsible, such as the hypervisor which provides isolation between tenants. VA should be able to review how the CSP met their controls, but will ultimately have to accept them or move to another CSP as the CSP may not be very flexible in meeting custom controls beyond FedRAMP
- **Lack of CSP diversity** – The FedRAMP process is costly and involved. GSA is working to improve the process, but in the interim the number of FedRAMP Compliant CSPs may be limited
- **FedRAMP Compliant CSP is not equal to VA Authorized CSP** – FedRAMP merely provides a process by which authorization information can be shared and reused. Although some controls will be inherited from the CSP, shared controls and VA controls must be addressed and an ATO requested from VA. The same ATO process used for internal systems applies with the addition of the ECSB to process CSP services

<u>FedRAMP Shared Controls</u>

It is important to understand the FedRAMP security controls model. The controls are grouped by control family designations and aligned to NIST 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, with a few exceptions:

- Not all controls are owned by a single owner. Controls are assigned to either the CSP, the organization or are shared. CSP controls are considered inherited

- There are additional controls and enhancements added by FedRAMP beyond NIST 800-53

The FedRAMP security controls required are based on the FIPS 199 system rating. Accordingly, there is a Low and Moderate baseline, and now, a High baseline.[3] As noted in the Shared Responsibility Model, the type of cloud hosting plays a role in which controls are shared. The CSP always maintains compliance up through the virtualization layer or hypervisor.

TABLE 3: SHARED RESPONSIBILITY MODEL

Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
User Access / Identity	User Access/Identity	User Access/Identity
Data	Data	Data
Application	Application	Application
Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization
Network	Network	Network
Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical

Customer Managed **CSP Managed**

Many CSPs highlight their focus and efficiency in securing the infrastructure through security controls and patching. The following are risks to consider when planning for VA security controls:

- **VA will retain responsibility for securing everything above the CSP level** - Except for the SaaS model; this will include different levels of patching on top of the CSP infrastructure. VA will also retain some of the same security challenges as hosting on premise, where misconfigurations, vulnerable coding, and unpatched vulnerabilities can create an attack surface
- **VA projects do not determine their own controls** – The required controls are set by VA policy via the ECSB to include any additional controls. These controls are being defined

[3] Please note the FedRAMP High baseline was published on June 23, 2016. There are approximately 100 additional controls beyond the Moderate baseline with a significant change being e-Authentication Level 4 required for all FedRAMP High systems. See control IA-5.

- **Higher security means higher cost** – Stakeholders should expect that FedRAMP High systems have a higher ongoing cost compared to Moderate or Low systems, which increases the importance of proper FIPS 199 ratings and not defaulting to a High rating unless justified
- **Coordinate shared controls with the CSP** – Connecting the CSP incident response processes to VA incident response processes is not plug and play. The use of multiple CSPs may add to the complexity
- **Verify CSP controls** – Two factor authentication (2FA) will not be of much use if a simple phishing email can gather enough information to contact the CSP Help Desk and have them disable 2FA due to a lost token. All CSPs have security controls to enforce isolation, but if these controls are not sufficient for the risk, VA may need to opt for dedicated resources. CSP security controls are documented as part of the FedRAMP Authorization Package. VA will need to review how these controls are met
- **Autoscaling and easier Instance Creation create risks** – VA governance regarding autoscaling and instance creation is important and may be more challenging than expected. The CSP does not differentiate between instances that should not be created; those no longer needed and approved ones. A lack of governance could create Shadow IT and unnecessary costs. Everyone can agree that autoscaling can be very beneficial for responding to an increase in users of an application. However, autoscaling to support increased resources for an incidence of malware in the cloud can put a very specific cost on the security lapse. Effective governance and monitoring of cloud activity is required to mitigate these risks. Service Delivery and Engineering (SDE) then establish and maintain image baselines for use in the cloud
- **The greater the number of CSPs the greater the effort to standardize controls** – Due to the proprietary approach many CSPs take to build their infrastructure, the implementation of a control that works well at one CSP may not translate well to another. The greater the number of CSPs, the greater the level of effort to build a secure reference architecture for each potential type of cloud deployment

3.3 Cloud Encryption

Cloud encryption may not be as straightforward as might be expected. FedRAMP already requires FIPS compliant algorithms for symmetric cryptography and FIPS 140-2 modules, but for media transport only. VA may be faced with architectural decisions or areas where a stronger encryption is available, but FIPS compliant is not an option.

- **Data in Use** - There are three areas of data exposure: data in transit, data at rest, and data in use. Encryption is currently available for data in transit and for data at rest. Data in use is data in memory or being processed. Where shared hardware is in

use, data in use requires VA to evaluate the CSP isolation controls. Because a CSP labels a cloud service for government does not mean tenants are restricted to federal agencies. If the isolation controls are not sufficient, dedicated resources may be the only remedy. Compute resources may account for most of cloud infrastructure costs. For a hybrid solution, resources could be stored in the cloud with compute executed in cleartext on premise

- **Key Control** – VA will consider data protected by encryption in instances where it retains the encryption keys. Whether or not the CSP uses their own layers of encryption, VA should use encryption where the keys are retained by VA and not the CSP whenever encryption is required. This mitigates the risk of accidental or intentional decryption of data by parties other than VA

3.4 Auditing of Cloud Services

All CSPs have monitoring tools. However, that is where some of the similarities end. Each CSP has their own set of tools which log different types of activity. To perform enterprise risk management, VA will need to import audit logs, especially if multiple CSPs are monitored. There are a few considerations for auditing beyond the need for a VA enterprise solution to ingest the data.

- Audit logging may not be mature – Some CSPs have tools in beta while some services may not have audit logs generated at all. As the service matures, the compatibility with the previous API and audit logs may change
- Export audit logs to ensure retention
- Scripting or 3rd party solutions may be required to create reporting
- Audit trails are provided at different time intervals depending on the CSP with some taking up to 15 minutes after the event occurs. Security event analysis may need to take this into account

<u>Auditing of Non-Compliant Cloud Projects</u>

As the ESCB is established and matured, VA will have a set of managed cloud services for projects. This will yield cost efficiencies and enable a common set of security controls, risk management, provisioning, support knowledge, maintenance, configuration management, and other management and support benefits. Some cloud projects are established outside of the ECSB, creating risk and decreasing efficiencies for VA. Identifying non-compliant projects presents a challenge as they are not centrally inventoried. To address this, the ECSB may use a combination of voluntary disclosure by project owners, electronic monitoring of VA network communications and external discovery to identify unofficial VA cloud projects for migration.

3.5 Cloud Availability

Availability is the third element of the well-known fundamental security triad of Confidentiality, Integrity and Availability (CIA). The cloud creates some similar challenges to outsourcing a data center except there is no hardware to pull if a change is made.

- **Cloud portability will create a risk for VA** – When OpenStack was released, it was expected to compete as an alternative to major CSPs, but that has yet to materialize as the open source project shifts its focus.[4] The market leaders in CSP all use different, proprietary methods to create cloud services. While host images and files are portable, the network infrastructure and security controls which support the services may not be. Recreating this at another CSP may not only incur costs, but take valuable time
- **Cloud availability is based on more than uptime –** Most CSPs offer options for logical and geographical redundancy to reduce the risk of service loss, but availability stretches beyond these areas. Having your private cloud vendor put their data centers up for sale can be a cause for concern. Multiple CSPs, strong companies in other areas, have closed their public cloud services. FedRAMP also creates the possibility of CSP decertification. Due to the differences between CSPs, VA faces a dilemma between avoiding vendor lock-in and maintaining cost efficiency in standardizing cloud controls. Some possible options to mitigate this risk include:
- Institute IAM SSOi as the default authentication protocol: SSOi shall become the default authentication protocol within VA to include privileged account management. Exception criteria will direct the use of direct PKI or Kerberos as required.
    - Maintain Disaster Recovery (DR) on premise – While the primary goal of migrating to cloud is the promise of lowering cost by decreasing hardware costs, on premise DR is one option for mitigating CSP problems. An internal cloud can reduce the footprint of the system when not in use
    - Maintain DR on another CSP – While this mitigates the risk, it still requires optimizing controls for an additional CSP which can increase costs
    - Maintain DR on the same CSP – Possibly the most cost effective method. Some agencies have simplified their cloud deployments by designing standard shared services within a single CSP such as IAM, centralized security, logging, scanning, patching, backup, archive and DR/COOP in a manner that new projects can plug in quickly. In this scenario, the agency's availability is tied to the health of the CSP
- Assign cloud monitoring – CSPs have created multiple services to allow clients to monitor cloud services. A primary reason for this is that the CSP is only responsible for

[4] http://www.theregister.co.uk/2016/01/21/openstack_goes_telecoms/

their infrastructure; VA will be responsible for monitoring services and collaborating with the CSP when necessary. A Network Operations Center (NOC) is recommended that can centrally monitor the WAN, CSP connectivity and cloud service alerts. Service Level Agreements (SLA) are also an important part of establishing monitoring services. Monitoring by individual stakeholders of just their own projects creates the risk of not seeing the big picture of network health and how different alerts may be related or signs of a more serious issue

3.6 Alignment to the One-VA Technical Reference Model (TRM)

All projects will leverage the approved tools and technologies located in VA's Technical Reference Model (TRM)[5] to comply with the architectural guidance provided in this document. Table 4 lists the approved tools for this EDP.

TABLE 4: LIST OF APPROVED TOOLS AND STANDARDS FOR CLOUD SECURITY

Technology Category	Example Technologies	Example Standards
Authentication	SiteMinder, Active Directory, CA Federation, Centrify Express, CyberArk, RSA Authentication Manager, Tivoli	X.509, OAuth/OpenID Connect, Kerberos, SAML, LDAP
Encryption	FIPS 140-2 compliant	WS-*, TLS per FIPS 140-2 requirements
Monitoring	CA User Activity Reporting Module, ElasticSearch Logstash, Microsoft System Center Operations Manager (SCOM), Splunk, SolarWinds Log and Event	Syslog Protocol (IETF RFC 5424), Transport Layer Security (TLS) Transport Mapping for Syslog (IETF RFC 5425)

3.7 Alignment to Veteran-Centric Integration Process (VIP)

VIP is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise. The VIP framework unifies and streamlines IT delivery oversight and will deliver IT products more efficiently, securely and predictably. VIP is the follow-on framework from Project Management Accountability System

[5] http://trm.oit.va.gov/

(PMAS) for the development and management of IT projects which will propel the Department with even more rigor toward Veteran-focused delivery of IT capabilities.

More information can be found at https://vaww.oit.va.gov/veteran-focused-integration-process-vip-guide/.

4 USE CASES

The following sections describe some general use cases that could apply to the use of a FedRAMP-compliant Cloud Service Provider for cloud services.

4.1 Healthcare Application on a Private Cloud

4.1.1 Purpose

The purpose of this use case is to discuss the impact to FISMA High rated systems that are currently using a private cloud solution.

4.1.2 Assumptions

- The solution is hosted at public CSP using PaaS
- The system is rated FISMA High due to Protected Health Information (PHI)
- The ECSB is still pending completion
- VA Cloud Security Policy is still pending completion

4.1.3 Use Case Description

1. The system owner is concerned about their health application. The FedRAMP High baseline sets new requirements for FISMA High systems in the cloud. The CSP which hosts the system is rumored to be considering the sale of their data centers which might be a deterrent to the investment required to become FedRAMP High compliant
2. VA policy does not yet address FedRAMP High systems, but the system owner needs to start planning in advance
3. The system owner identifies several risks related to the current system design:
    a. Encryption keys are controlled by the CSP
    b. Audit logs are accessed through the CSP portal where they are deleted based on CSP policy and not retained by VA
    c. The system is designed for high availability, but does not have a viable disaster recovery plan in place if the CSP loses FedRAMP certification
    d. The system allows username and password authentication and does not use e-Authentication Level 4 required by FedRAMP High

4. The system owner is able to engage in advance with other VA internal organizations to determine how to address the identified gaps and evaluate other CSP options should the system need to change hosting

4.2 VA Website Hosting General Information on a Medical Condition

4.2.1 Purpose

The purpose of this use case is to discuss the cloud requirements for a VA website hosting information that is not sensitive.

4.2.2 Assumptions

- The project is already hosted at a CSP
- Cloud services were established before VA developed cloud policies
- The project was not tracked along with other cloud projects for compliance

4.2.3 Use Case Description

1. A VA website hosted by a CSP was flagged by GAO for not implementing recommended cloud best practices
2. VA is reviewing the system ATO to determine if the proper controls are in place
3. Areas of risk identified:
    a. The service provided by the CSP is not FedRAMP certified
    b. Users are connecting to the website without traversing the VA TIC
    c. The contract is not compliant with current VA policy
4. The system owner is reviewing options for moving the website to a FedRAMP Low compliant service but wants to know why TIC compliance is required
5. As part of the authorization review, the website information is considered restricted data. The justification is that the data presented represents VA practices and recommendations and reflects on VA's reputation. TIC compliance provides protection for the website against unauthorized access to include defacement and denial of service attacks

4.3 Information Sharing Website and Blog Migration to the Cloud

4.3.1 Purpose

The purpose of this use case is to discuss the cloud requirements for a VA website designed to allow external projects teams to build websites and blogs for sharing information with VA on

new and innovative ideas such as Electronic Health Record (EHR) data elements, patient identification techniques, VA app extensions and others.

4.3.2 Assumptions

- The project is already hosted at a CSP
- Cloud services were established before VA developed cloud policies
- The FISMA rating for the system is Moderate
- The established ECSB guides cloud projects

4.3.3 Use Case Description

1. A system owner for a VA website heard of the changing requirements related to cloud controls and is concerned his project may be non-compliant
2. The system owner contacts the ECSB for more information
3. Upon a review of the system, the restricted data is identified as VA email addresses and generally public information
4. The ECSB recommends an authorization review to categorize the system as FISMA Low. This corresponds to the data sensitivity level and provides cost savings. The ECSB recommends migrating the site to a new CSP where VA established a FedRAMP Low zone and achieves better cost savings due to volume purchasing across multiple projects

APPENDIX A. SCOPE

A Cloud Security Model sets standards for what systems or information can be handled in a cloud environment, the type of cloud model required based on the sensitivity level and the baseline requirements to ensure VA auditing, security monitoring, privacy/record management, data ownership, and all compliance requirements are met. This EDP will define an enterprise cloud security model that starts with the use of Federal Risk and Authorization Management Program (FedRAMP) approved providers and addresses the additional requirements beyond FedRAMP. This model will help stakeholders to meet VA requirements when reviewing cloud options for their solution or service.

- Initial focus on TIC compliance and auditing of cloud resources
- Addresses cloud security objectives in VA's Enterprise Cybersecurity Strategy
- ETSP establishes IT vision consisting of cloud-based services
- Cloud strategy impacts the security standards required for a cloud solution
- Align VA's cloud security paradigm with Federal mandates and VA policies
- Does not address virtualized hosting within VA data centers
- While the EDP reviews Auditing, Authentication and DR/COOP considerations for cloud, see the EDPs related to those areas for more information

Document Development and Maintenance

This EDP was developed collaboratively with internal stakeholders from across the Department and included participation from VA's Office of Information and Technology (OI&T), Enterprise Program Management Office (ePMO), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). Extensive input and participation was also received from VHA, VBA and NCA. In addition, the development effort included engagements with industry experts to review, provide input, and comment on the proposed pattern. 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

This appendix provides definitions for terms used in this document, particularly those related to databases, database management, and data integration.

Key Term	Definition
Access	Interaction with a computer system for instance VistA. Such interaction includes data retrieval, editing (create, update, delete) and may result from a variety of technical mechanisms including traditional user log on, consuming applications exercising middleware based connectivity, SOA service requests, et cetera.
Accurate, unambiguous user identity	Information that represents the actual human that is interacting with a computer system, including the initiation of that interaction.
Application proxy	Construct involving the use of a generic, non-human "user" entity to represent "machine-to-machine" interaction where appropriate for interactions that do not involve a specific end user.
Auditing	The inspection or examination of an activity based on available information. In the case of computer systems, this is based on review of the events generated by the system or application.
Consuming application	The application consuming services from a provider system. Generally used when discussing a front-end application supporting a user, but even service providers can themselves be a consumer of other services.
Delegated Access	When an owner authorizes another to serve as his or her representative for access to a particular resource.
Enterprise Service Bus (ESB)	An SOA infrastructure device which manages message traffic, routing and a variety of other functions for instance orchestration, mediation, etc. The primary ESB at VA is the Enterprise Messaging Infrastructure (eMI).
Enterprise Shared Service (ESS)	A SOA service that is visible across the enterprise and can be accessed by users across the enterprise, subject to appropriate security and privacy restrictions.

Key Term	Definition
Identity attributes	Characteristics which describe the user (e.g. name, National Provider Identifier, organization, etc.). Establishment of reasonably reliable "unique identity" is generally based on a combination of multiple identity attributes. Specific user identifiers include employee number and email address; may vary from organization to organization but identifier types ought to remain constant for all transactions from a specific organization.
Machine-to-machine interaction	In some cases, application processes resulting from workflow (not human interaction) will result in interaction with provider systems to download data, initiate background processing, etc. These actions are not directly initiated by a specific human and the interaction would be attributed to an application, possibly via a service account.
OAuth 2.0	An open standard for authorization which provides clients a method to delegate access to server resources on behalf of a resource owner without sharing user credentials. OAuth 2.0 is not backwards compatible with OAuth 1.0.
Provider system	A system (e.g. VistA) which provides service at the request of a consuming application.
Representational State Transfer (REST)	An architecture style for designing client-server communications which is stateless and provides a uniform interface to access named resources using interconnected resource representations.
SAML token	An XML-based open standard data format for exchanging authentication and authorization data between parties.
System for Cross-Domain Identity Management (SCIM)	The SCIM Protocol is an application-level, REST protocol for provisioning and managing identity data on the web as described by IETF RFC 7642.
Service Oriented Architecture	A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations
User	A person who interacts with a computer system application. In this context, a "user" is not limited to VA staff members and may include persons from external organizations, patients, beneficiaries, designees, etc.
SSO and User Provisioning	A services provided by Identity and Access Management (IAM) for authenticating users and providing user provisioning information to other systems.

Key Term	Definition
User types	Traditional types including VA staff, staff of non-VA agencies (e.g. DoD), staff of private sector organizations (e.g. Walgreens), nontraditional, non-staff types including patients, beneficiaries, designees, sponsors, caregivers, etc.

APPENDIX C. ACRONYMS

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

Acronym	Description
AD	Active Directory
ADFS	Active Directory Federated Services (SSO based on SAML/WS-*)
API	Application Program Interface
ASD	Architecture, Strategy and Design
CSP	Credential Service Provider
ECSB	Enterprise Cloud Services Broker
eMI	Enterprise Messaging Infrastructure
ESB	Enterprise Service Bus
ESS	Enterprise Shared Service
FedRAMP	Federal Risk and Authorization Management Program
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HIPAA	Health Insurance Portability and Accountability Act
HTTPS	Hypertext Transfer Protocol over TLS
IAM	Identity and Access Management
IETF	Internet Engineering Task Force
IdP	Identity Provider
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
PCI	Formally known as Payment Card Industry Data Security Standard (PCI-DSS)
PKI	Public Key Infrastructure
PIV	Personal Identity Verification
REST	Representational State Transfer
RFC	Request for Comment
RPC	Remote Procedure Call
SAML	Security Assertion Markup Language
SCIM	System for Cross-Domain Identity Management
SDD	System Design Document
SLA	Service Level Agreement
SPML	Service Provisioning Markup Language
SOA	Service-Oriented Architecture
SRG	Security Requirements Guide
SSOe/SSOi	Single Sign-On External/Internal
TLS	Transport Layer Security

Acronym	Description
TRM	Technical Reference Model
VHA	Veteran Health Administration
VistA	Veterans Health Information Systems and Technology Architecture
XML	Extensible Markup Language

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES

This EDP is aligned to the following VA OI&T references and standards applicable to all new applications being developed in the VA, and are aligned to the VA Enterprise Technical Architecture (ETA):

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
1	VA	VA Directive 6551	Establishes a mandatory policy for establishing and utilizing Enterprise Design Patterns by all Department of Veterans Affairs (VA) projects developing information technology (IT) systems in accordance with VA's Office of Information and Technology (OI&T) integrated development and release management process, the Veteran-focused Integration Process (VIP).
2	VA OIS	VA 6500 Handbook	Directive from the OI&T OIS for establishment of an information security program in VA, which applies to all applications that leverage ESS.
3	VA	VA Strategy Lockdown VAIQ#7641464	VA Strategy for Adoption of Cloud Computing (draft)
4	VA IAM	VA Directive 6051	Department of Veterans Affairs Enterprise Architecture (VA EA), July 12, 2002
5	VA	VA Handbook 6517	Risk Management Framework for Cloud Computing Services (draft)
6	NIST	NIST SP 500-291	NIST Cloud Computing Standards Roadmap, Version 2, July 2013
7	NIST	NIST SP 500-292	NIST Cloud Computing Reference Architecture
8	NIST	NIST SP 800-145	The NIST Definition of Cloud Computing, NIST SP 800-145, Sept. 2011
9	NIST	NIST SP 500-299	NIST Cloud Computing Security Reference Architecture
10	DoD	DoD Cloud Computing Security Requirements Guide (SRG) Version 1 Release 2	Department of Defense Cloud Computing Strategy
11	GSA	GAO 14-753	Describes cloud computing challenges 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	Policy, Directive, or Procedure	Purpose
12	OMB	OMB M-08-05, Implementation of Trusted Internet Connections (TIC)	Establishes TIC to optimize and standardize the security of external network connections for Federal agencies.
13	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.
14	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.
15	Federal	FIPS 199	FIPS 199 (Federal Information Processing Standard Publication 199)
16	Federal	FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
17	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.
18	GSA	FedRAMP Security Assessment Framework	Establishes required controls and enhancements for cloud computing based on the FIPS 199 rating of the system. Controls are grouped by control family designations and aligned to NIST 800-53. See https://www.fedramp.gov/ for more information.

APPENDIX E. CLOUD SECURITY SAMPLE ARCHITECTURE

The sample architecture below is not a reference architecture. It is simply an example of how the cloud security risks discussed in the EDP might be addressed in the cloud to generate discussion. The scope is restricted to cloud security areas. A full reference architecture will be created and maintained under the guidance of the ECSB.

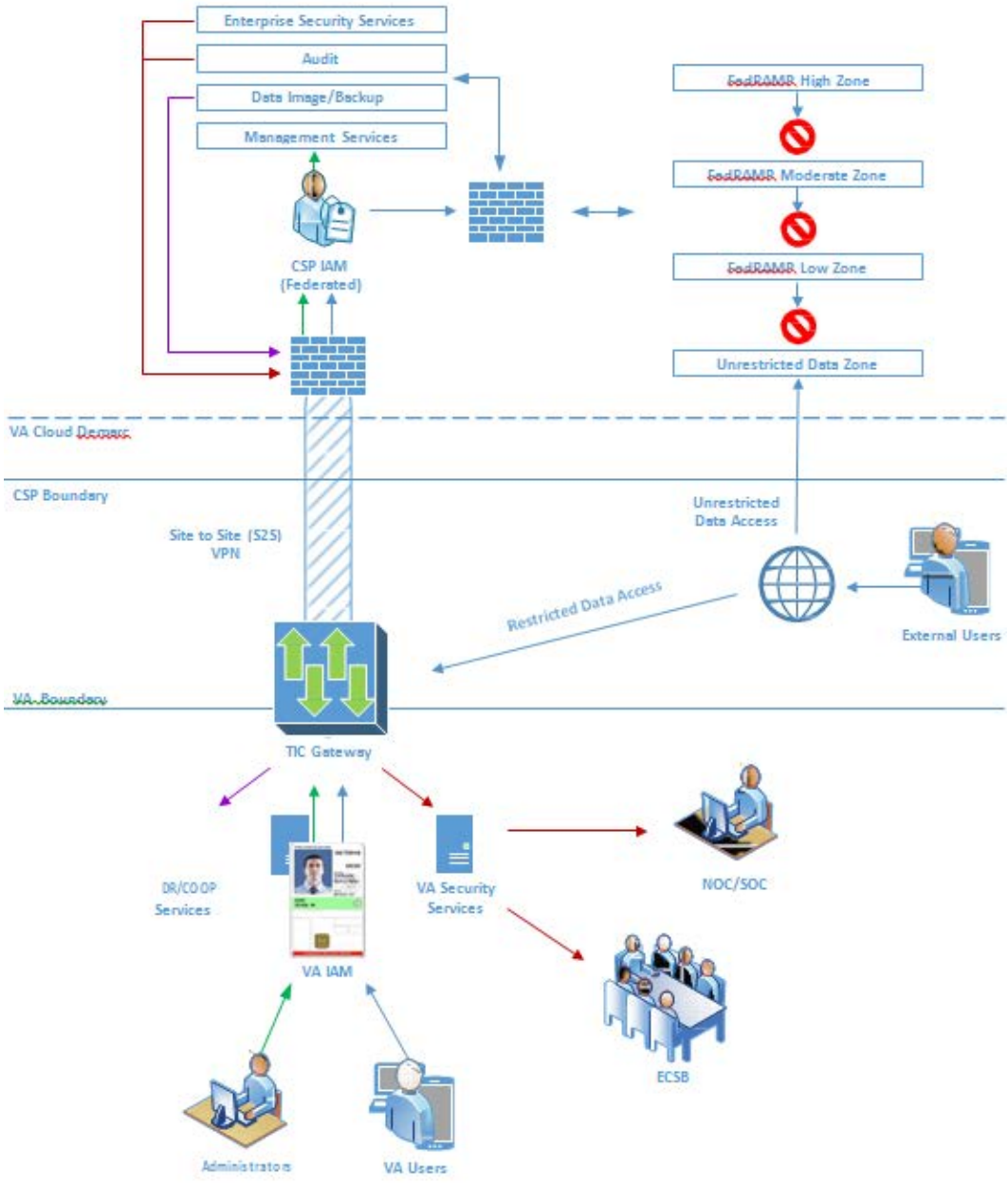

FIGURE 3: SAMPLE CLOUD SECURITY ARCHITECTURE OVERVIEW

The image below shows additional details within the Virtual Private Clouds (VPC) for security services and the FedRAMP High zone

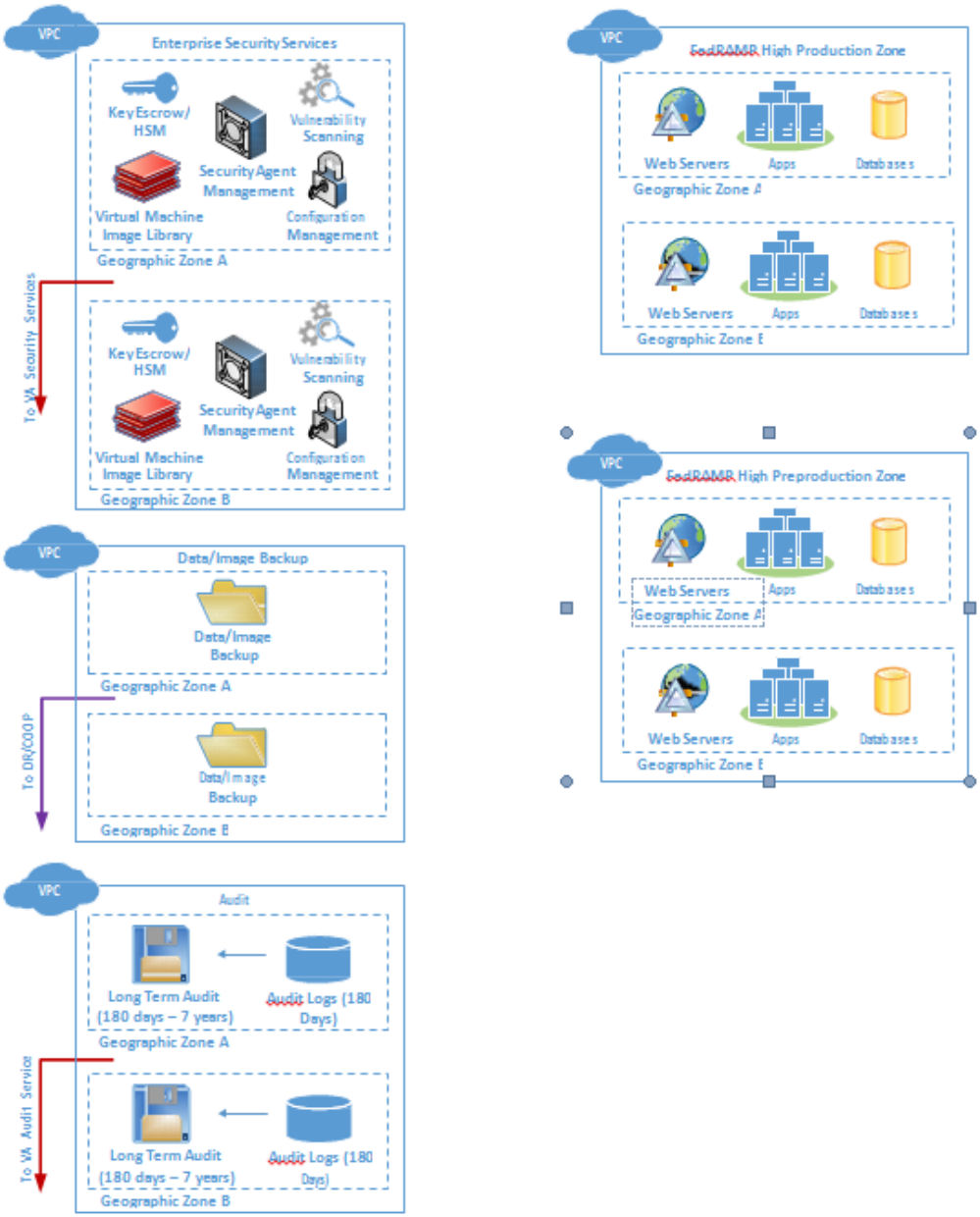

FIGURE 4: CLOUD SECURITY SAMPLE ARCHITECTURE VPC HIGHLIGHTS

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.