DEPARTMENT OF VETERANS AFFAIRS
Washington, DC 20420

VA HANDBOOK 6517
Transmittal Sheet
November 15, 2016

RISK MANAGEMENT FRAMEWORK FOR CLOUD COMPUTING SERVICES

1. **REASON FOR ISSUE:** To establish policy requirements and responsibilities for the Department of Veterans Affairs (VA) to ensure compliance with Federal Risk and Authorization Management Program (FedRAMP) Assessment and Authorization (A&A) and continuous monitoring requirements for cloud computing services.

2. **SUMMARY OF CONTENTS/MAJOR CHANGES:** This handbook provides policy requirements and responsibilities for categorizing, identifying, selecting, assessing, authorizing, and monitoring cloud computing services using the FedRAMP. This handbook supports VA Directive 6517, *Cloud Computing Services* and the Department-wide compliance with the Federal Information Security Modernization Act of 2014 (FISMA), 44 United States Code (U.S.C.) §§ 3541 *et seq.,* , 38 U.S.C. §§ 5721-5728, and the security of VA information and information systems administered by VA, or on behalf of VA.

3. **RESPONSIBLE OFFICE:** The Office of the Assistant Secretary for Information and Technology (005), Information Security (005R), Office of Cyber Security (005R2) is responsible for the content contained in this handbook.

4. **RELATED DIRECTIVE:** VA Directive 6517, Cloud Computing Services; VA Directive 6500, Managing Information Security Risk: VA Information Security Program; VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program; VA Handbook 6500.3, Assessment, Authorization, and Continuous Monitoring of VA Information Systems; VA Handbook 6500.5, Incorporating Security and Privacy into the System Development Life Cycle; and VA Handbook 6500.6, *Contract Security*.

5. **RESCISSIONS:** NONE.

CERTIFIED BY:

/s/

LaVerne H. Council
Assistant Secretary for Information and Technology and Chief Information Officer

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/

LaVerne H. Council
Assistant Secretary for Information and Technology and Chief Information Officer

Distribution: Electronic Only

This page is intentionally blank for the purpose of printing front and back copies.

RISK MANAGEMENT FRAMEWORK FOR CLOUD COMPUTING SERVICES

CONTENTS

PARAGRAPH **PAGE**

ENTER DOCUMENT TITLE HERE

CONTENTS

PARAGRAPH **PAGE**

APPENDICES **PAGE**

FIGURES **PAGE**

RISK MANAGEMENT FRAMEWORK FOR CLOUD COMPUTING SERVICES

1. PURPOSE

This handbook establishes policy requirements and responsibilities for cloud computing services to ensure compliance with VA Handbook 6500, Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), and Federal Risk and Authorization Management Program (FedRAMP) Assessment and Authorization (A&A) and continuous monitoring requirements.

2. SCOPE

The requirements in this handbook apply to all VA Operating Units, contractor-operated services, third party assessment organizations (3PAO), cloud service providers (CSP), and cloud brokers. This includes associated information resources located and operated at contract facilities and resources located and operated at other government agencies that support VA mission requirements or VA authorized activity in conjunction with cloud services.

3. OVERVIEW

a. The Federal Chief Information Officer (CIO) has established FedRAMP to provide a standard approach to A&A (formerly Certification & Accreditation) of cloud computing services, and has directed NIST to serve as the technical advisor for assessing risks in implementation of cloud computing solutions. The FedRAMP portal at cloud.cio.gov/FedRAMP describes the FedRAMP process and procedures, and contains templates for agencies to use.

b. There are three primary cloud service models available:

(1) Software as a Service (SaaS) - The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

(2) Platform as a Service (PaaS) - The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

(3) Infrastructure as a Service (IaaS) -The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

c. There are four cloud deployment models: Public Cloud; Private Cloud; Community Cloud; and Hybrid Cloud. Public Cloud, Community Cloud, and Hybrid Cloud deployments cannot be used for VA restricted data currently.

(1) Public Cloud - A "public" cloud service is available to the general public over the Internet. An agency may choose to outsource the system to a CSP where it would be deployed at the CSPs facility; or collocated at the agency's data center and provide access through the agency's Internet Gateways. Agency personnel access the service through the Internet Gateways from the agency's Intranet. Public cloud deployments must be documented in FedRAMP and require a FedRAMP Authorization to Operate (ATO).

(2) Private Cloud - A "private" cloud service is operated solely for a single organization or agency.

(a) If outsourced and deployed at the CSPs facility, the CSP dedicates specific cloud services to that agency and no other clients. Private cloud deployments in the CSPs facility must be documented in FedRAMP.

(b) An agency may also deploy a private cloud solution at their data center, connected to and accessed by agency personnel through the agency's Intranet. Private cloud resources are only shared within an agency and not with external entities. Access by the public via the Internet is not allowed; however agency personnel may have remote access to an Agency's Intranet and private cloud service via the Agency's Internet gateway using approved remote access technology.

(c) FedRAMP is not required for private cloud services that are only used by the agency; and located in a Federal facility; and do not provide cloud services to any external entities. Information systems exempt from FedRAMP must still comply with VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program* and Federal Information Security Modernization Act of 2014 (FISMA) requirements and the appropriate NIST security standards and guidelines for their private cloud-based information systems.

(3) Community Cloud - A "community" cloud service may be procured and operated by one or more agency or organization that shares specific interests or needs; such as security, compliance, or jurisdiction considerations. The agencies or CSP may manage the community cloud; which may be on-premises at an agency's facility or off-premises at the CSP's facilities. The same security measures and requirements as

private clouds may apply. Access to this service would be restricted to community participants. Community cloud deployments must be documented in FedRAMP and require a FedRAMP ATO.

(4) Hybrid Cloud - A "hybrid" cloud comprises two or more clouds (Private Cloud, Public Cloud, or Community Cloud) and may include a mix of both internally and externally hosted services. Hybrid cloud deployments must be documented in FedRAMP and require a FedRAMP ATO.

4. FEDRAMP PROCESS AND SECURITY ASSESSMENT

a. The FedRAMP process (identified in the figure 1 below) is compliant with FISMA and is based on NIST Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

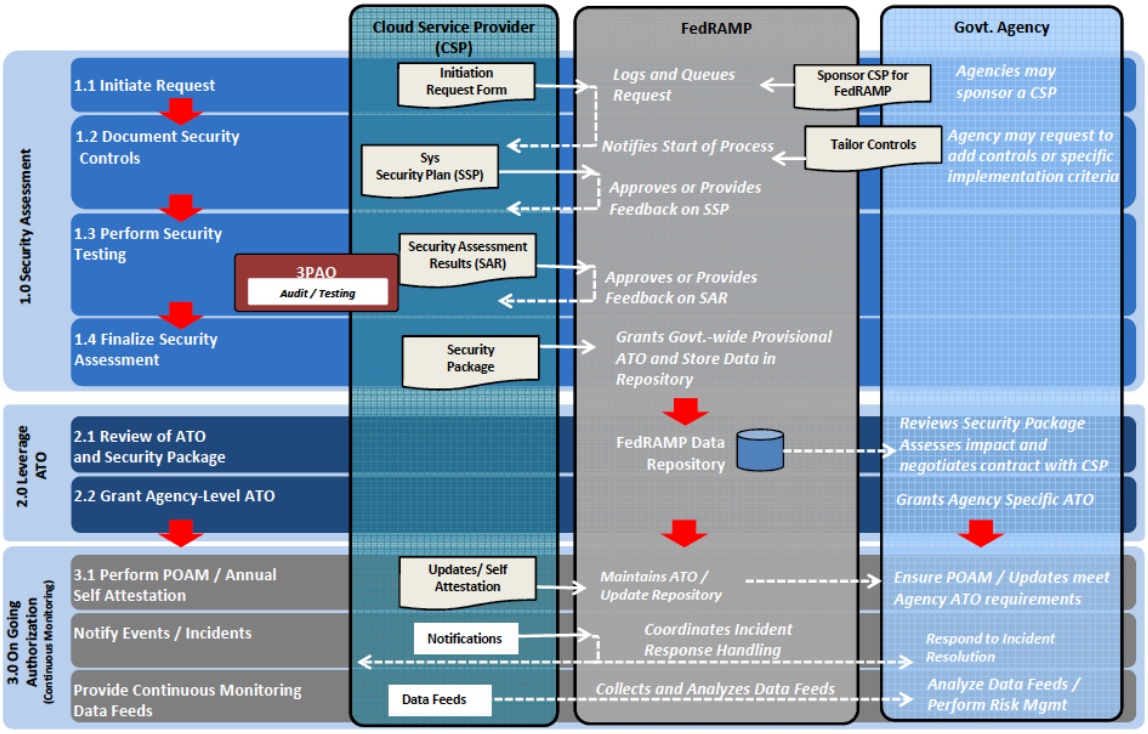

Figure 1: FedRAMP Process Overview

b. Federal agencies, CSP, and 3PAO will use FedRAMP differently, but must all understand and use the FedRAMP security controls baseline and requirements. These requirements include using FedRAMP templates, test cases, and ongoing Assessment and Authorization processes. FedRAMP Stakeholders include:

(1) Agency Cloud Consumer – Federal Agency utilizing cloud computing services;

(2) Cloud Service Provider (Either commercial or Federal agency operator) – Provides cloud computing services;

(3) FedRAMP Joint Advisory Board - Performs risk authorization and grants the provisional ATO;

(4) General Services Administration FedRAMP Program Management Office (PMO) – Responsible for operational management of FedRAMP;

(5) Third Party Assessment Organization (3PAO) - Independently performs security assessments of CSP systems and creates security assessment package artifacts in accordance with FedRAMP requirements.

5. POLICY AND PROCEDURES

a. Step 1: Categorize the Information System

FedRAMP has defined the security control baseline for low and moderate impact level systems as defined by Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. These security controls were selected from the NIST catalog of controls and enhancements as described in Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4.

(1) VA is responsible for categorizing the information and information system in accordance with Handbook 6500, *Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program*. The processes and tasks that will be performed in this step are:

(a) Conduct Impact Analysis to categorize the system;

(b) Conduct Business Impact Analysis (BIA); and

(c) Conduct Privacy Threshold Analysis (PTA).

b. Step 2: Approve Business Use Case

All VA cloud technology implementations must receive VA CIO approval of their business use case prior to acquisition of a cloud technology solution and subsequent A&A approval based on satisfying all VA security requirements. This approval requires a business use case submission which provides basic information on the model and a preliminary cost-benefit analysis (see Appendix A). The VA CIO must report annually to the Federal CIO, the number of cloud submissions reviewed, approved, and disapproved. Additional guidance on business use cases can be found on the Enterprise Operations Cloud Services Portal.

(1) Service Delivery and Engineering (SDE) will conduct a feasibility review based on SDE’s cloud technology standard operating procedures upon receipt of a

business use case from the business owner. If SDE determines that the requirements are best suited for a cloud service, SDE will initiate a preliminary cost-benefit analysis for the implementation. SDE will maintain an inventory of all reviewed business use cases (approved and disapproved) for the VA CIO's required annual report to the Federal CIO.

(2) The preliminary cost-benefit analysis is a preliminary estimate and will include software and hardware cost reduction rationale, any relevant data consolidation considerations, and any decommissioning costs for a legacy system, if applicable, including repurposing costs to move to a cloud service. Records management functions and retention and disposition requirements must be fully incorporated into information life cycle processes and stages, including the design, development, implementation, and decommissioning of information systems, particularly Internet resources to include storage solutions and cloud-based services such as software as a service, platform as a service, and infrastructure as a service. Information that the CIO would use to consider approval of the business use case is contained in the cost-benefit analysis.

(3) Upon completion of the preliminary cost-benefit analysis, SDE will forward the business use case and the cost-benefit analysis to the VA CIO for his review.

(4) The VA CIO will review the business use case, the preliminary cost-benefit analysis, and feasibility review and either approve the business use case for development, disapprove the business use case for development, or approve the business use case for development with contingencies.

(5) The VA CIO will return approved business use cases to SDE for in-house or outsourced development. SDE will provide approved business use cases to the appropriate Office of Information and Technology (OI&T) office or team to proceed with development for approved cloud services using appropriate VA system development and contracting procedures.

(6) The VA CIO will return disapproved business use cases to the business owner. The business owner may submit a request for reconsideration with cost/benefit substantiation and rationale for approval. If approved, the business use case may proceed to development handling through SDE.

(7) The VA CIO will return business use cases that have been approved with contingencies to the business owner with criteria for receiving approval based on modification and cost-benefit substantiation. When contingencies have been reviewed and addressed, the business owner will resubmit the business use case through SDE for review/approval.

(8) Connections to the cloud must meet the requirements in the Department of Homeland Security (DHS) Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 and VA Handbook 6500. A TIC between any cloud platform at the CSPs facility and an agency's enterprise network is required.

c. **Step 3: Identify Security Requirements**

VA is responsible for identifying the security requirements for the information system. The processes and tasks that will be performed in this step include:

(1) Conduct a Risk Assessment;

(2) Select the baseline security controls; and

(3) Conduct a Confidentiality, Integrity, and Availability analysis.

d. **Step 4: Select the Cloud Service**

(1) FedRAMP is mandatory for cloud computing services which consist of one or more deployment models (Public Cloud, Community Cloud, Private Cloud, or Hybrid Cloud), and one or more service models (IaaS, PaaS, or SaaS) at the low, moderate, or high risk impact levels. Cloud computing services may be located within one or more Federal or commercial facilities to meet agency objectives.

(2) **VA is responsible for determining the deployment model and service model for the information** system. The tasks that will be performed in this step are:

(a) Determine if the information system will be deployed in a Private Cloud, Community Cloud, Public Cloud, or Hybrid Cloud.

(b) Determine if the service platform will be provided as SaaS, PaaS, or IaaS.

(3) The level of control VA has over the cloud environment and the roles and responsibilities of the agency and cloud service provider will be different depending on the deployment and service model used for the cloud service. Figure 2 below shows how the responsibilities and ownership are shifted from the agency to the cloud service provider depending on the different cloud deployment models. The color blue in the figure represents VA's level of responsibility, and the color green represents the CSP's responsibilities.

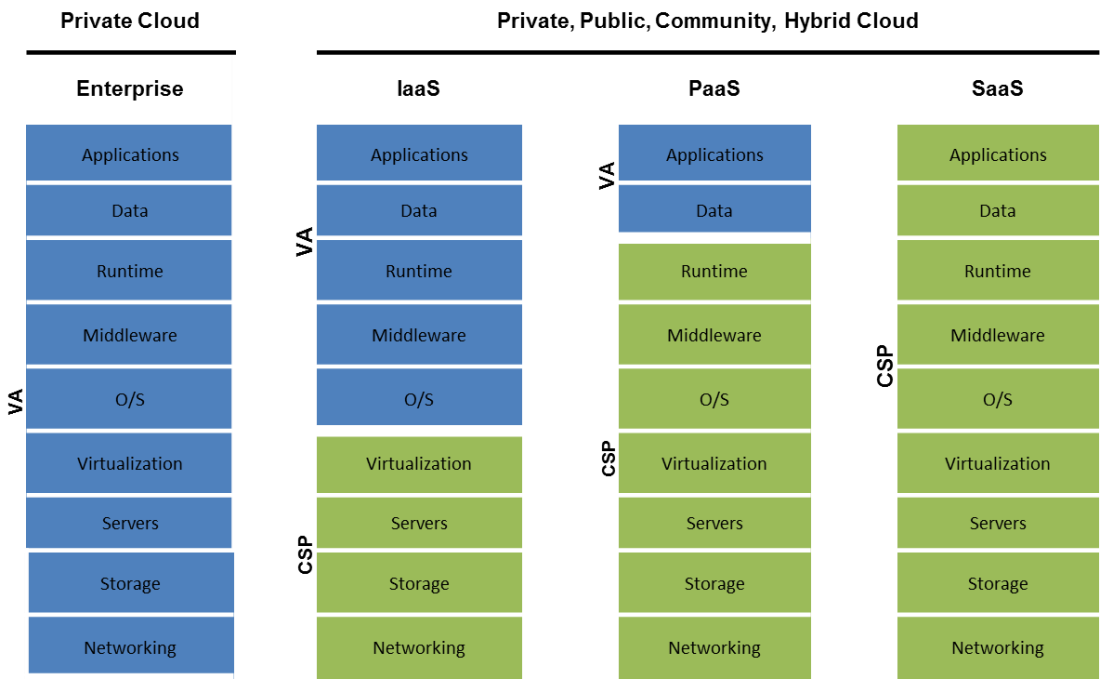

Figure 2: Level of Control in Cloud Environments

(4) In a traditional enterprise deployment (represented in the left-most stack of the diagram), the agency is fully responsible for the information system purchased and deployed in their facility. All hardware and software, with the exception of leased products, are information technology assets owned by VA for the life of the information system.

(5) In a cloud service environment, the facility and infrastructure is typically owned and operated by the cloud service provider in all three service models – IaaS, PaaS, and SaaS. In Figure 2, ownership and responsibility above the infrastructure layer differs depending on the service model being used.

e. **Step 5: Assess Service Provider(s)**

(1) VA is responsible for determining if a CSP already has a FedRAMP provisional authorization for a deployment model and service model that VA can leverage.

(2) There are three methods for complying with FedRAMP, as described below:

(a) **Leverage FedRAMP Provisional Authorization** - FedRAMP Provisional Authorizations are given to security authorization packages that have gone through the FedRAMP assessment process and are authorized by the FedRAMP Joint Authorization Board (JAB). Leveraging an existing FedRAMP Provisional Authorization

is the quickest way for VA to comply with FedRAMP requirements. In order to receive a JAB Provisional Authorization, CSPs must be assessed by an accredited 3PAO to independently validate and verify that they meet FedRAMP security requirements. To leverage an existing Provisional Authorization VA shall:

1. Select the FedRAMP approved security authorization package to review and submit a Package Access Form;

2. Review the security assessments packages in the FedRAMP repository including the application of security control implementation, and evidence of the CSPs implementation of these controls;

3. Review existing vulnerabilities and risk mitigation plans for the cloud service represented by the package. Results are documented in Cloud Security Assessment Report (CSAR);

4. Understand the control responsibility identified in the Control Implementation Summary (CIS). Results are documented in CSAR;

5. Tailoring of security controls may be required to meet VA security requirements;

6. Negotiate a contract with the CSP and include the appropriate contract language from FedRAMP and VA Handbook 6500.6*, Contract Security*, as appropriate; and

7. After reviewing the security assessment package and Provisional Authorization, the VA Authorizing Official can decide to grant the VA ATO.

(b) **Use Existing VA Authorization to Operate** - If VA decides to act as a CSP and use a cloud service that is not in the FedRAMP repository, the FedRAMP process must be used including:

1. VA must ensure all FedRAMP templates comply with all current guidance, and submit the documentation to FedRAMP;

2. VA must assign and use a VA Information Security Officer (ISO);

3. VA must ensure updates to the CSP authorization package are provided to the FedRAMP PMO according to the required frequency;

4. If VA does not use a FedRAMP 3PAO for audit and testing, VA shall submit an attestation describing the independence and technical qualifications of the 3PAO utilized to assess the CSP package; and

5. Any VA ATOs that have not been audited and tested by a FedRAMP 3PAO will not be eligible for JAB review and provisional authorization.

(c) **Assess a CSP for VA Agency Authorization** - If the CSP does not have a FedRAMP provisional or agency authorization, VA can assess the CSP solution using the FedRAMP documents and process, to include:

1. The cost for FedRAMP assessment and authorization is the CSPs responsibility;

2. The CSP must use all FedRAMP templates and guidance and submit documentation to FedRAMP;

3. VA must assign and use VA ISOs;

4. Negotiate a contract with CSP and include the appropriate contract language from FedRAMP and VA Handbook 6500.6, *Contract Security*, as appropriate;

5. CSPs are required to use an accredited 3PAO to independently validate and verify that they meet FedRAMP security requirements; and

6. Ensure updates to the CSP authorization package are provided to the FedRAMP Program Management Office (PMO) as required.

f. **Step 6: Authorize the Use of the Selected Cloud Provider**

(1) If leveraging a FedRAMP Provisional Authorization, the CSP will primarily be responsible for performing the steps to obtain the FedRAMP provisional ATO from the JAB. The CSP is also primarily responsible for performing the steps necessary to obtain a VA FedRAMP Agency ATO, up to and including ensuring an appropriate assessment is performed on behalf of VA.

(2) The steps for FedRAMP assessment and authorization are:

(a) Document Service Boundary and Assets by submitting the FedRAMP Initiation Request Form to FedRAMP. The FedRAMP request form is used by Federal agencies and CSPs to request initiation of the FedRAMP security assessment process;

(b) Identify Impact Level and submit FIPS 199 Worksheet to FedRAMP. The FIPS 199 Security categorization is used to determine the impact level to be supported by the cloud service;

(c) Tailor Controls and submit Control Tailoring Workbook (CTW) to FedRAMP. This document is used by CSP to document their control implementation and define their implementation settings for FedRAMP defined parameters and any compensating controls;

(d) Define Controls Implementation and submit Control Implementation Summary to FedRAMP. This document summarizes the control ownership and indicates which controls are owned and managed by the CSP and which controls are owned and managed by the leveraging agency;

(e) Submit System Security Plan (SSP) to FedRAMP. The SSP describes how the controls are implemented within the cloud information system and its environment of operation. The SSP is also used to describe the system boundaries;

(f) Submit CSP Information Security Policies to FedRAMP which governs the system described in the SSP;

(g) Submit Agency User Guide to FedRAMP which describes how leveraging agencies use the system;

(h) Submit CSP Rules of Behavior which defines the rules that describe the system user's responsibilities and expected behavior with regard to information and information system usage and access;

(i) Submit IT Contingency Plan to FedRAMP. These documents define and test interim measures to recover information system services after a disruption. The ability to prove that system data can routinely be backed up and restored within agency specified parameters is necessary to limit the effects of any disaster and the subsequent recovery efforts;

(j) Submit Configuration Management Plan to FedRAMP which describes how changes to the system are managed and tracked. The Configuration Management Plan should be consistent with NIST SP 800-128;

(k) Submit Incident Response Plan. This plan documents how incidents are detected, reported, and escalated and should include timeframes, points of contact, and how incidents are handled and remediated. The Incident Response Plan should be consistent with NIST Special Publication 800-61;

(l) Submit E-Authentication Workbook to FedRAMP to indicate what authentication level (1-4) will be used in the cloud system. The E-Authentication Workbook defines the level in terms of the consequences of the authentication errors and misuse of credentials, and is used to complete a risk assessment and map identified risks;

(m) Submit Privacy Threshold Analysis to FedRAMP to help determine if a Privacy Impact Assessment is required;

(n) Submit Privacy Impact Assessment to FedRAMP. This document assesses what Personally Identifiable Information (PII) is captured and if it is being properly safeguarded. This deliverable is not always necessary depending on the outcome of the Privacy Threshold Analysis;

(o) Submit 3PAO Designation Form to FedRAMP. The CSP submits this form to FedRAMP in order to designate the FedRAMP accredited 3PAO that will perform an independent assessment of the controls protecting the CSP’s system. In the case of a

VA assessor not being a 3PAO (in support of a VA A-ATO), an attestation to their sufficient independence is submitted;

(p) Develop Testing Plan and submit Security Assessment Plan (SAP) to FedRAMP. The SAP describes the scope of the assessment including: Security controls and control enhancements under assessment using the FedRAMP security control baseline; Use of FedRAMP Assessment Test Procedures to determine security control effectiveness; and Assessment environment, assessment team, and assessment roles and responsibilities;

(q) Audit Control implementations and submit Security Assessment Report (SAR) to FedRAMP. The SAR is used to document the overall status and deficiencies in the security controls. The SAR serves as the basis document that the JAB will utilize to guide their Provisional Authorization decision, if applicable, and shows security weaknesses that will be mapped to corresponding Plan of Actions and Milestones (POA&M) items. In situations where a security control cannot be successfully implemented through standard practice or a compensating control, it will be considered a residual risk;

(r) The 3PAO, or independent assessor, will perform Vulnerability Testing;

(s) Submit Security Assessment Test Cases which identify the test procedures that have been tailored for FedRAMP. These test cases are captured in the form of an Excel Workbook and are based on NIST SP 800-53A;

(t) Develop and submit POA&M s to FedRAMP which describes the CSP's specific tasks and timelines for remediating or changing system or control specific implementations;

(u) CSP will submit Supplier's Declaration of Conformity (SDOC) to verify and attest to the truth of the implemented security controls as detailed in their assessment package;

(v) Compile all updated and final documentation and submit Security Assessment Package to FedRAMP;

(w) Review clarification questions from FedRAMP and answer questions from Perform Final Risk Assessment; and

(x) Receive FedRAMP Findings Summary from FedRAMP and accept the document findings and make any updates to POA&M.

(3) VA is responsible for:

(a) Reviewing the Provisional Authorization Letter from FedRAMP and accepting the Provisional Authorization; and

(b) Grant a VA ATO.

g. **Step 7: Monitor the Cloud Provider**

(1) Ongoing A&A (Continuous Monitoring): Provides automated data feed application programming interfaces for key controls; coordinates government response to security incidents and events at cloud systems; performs annual review of cloud systems for compliance through self-attestation.

(2) The FedRAMP ongoing Assessment and Authorization program is based on NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organization.

(3) Once a FedRAMP Provisional Authorization and a VA ATO for a cloud system has been granted, implement an ongoing Assessment and Authorization (continuous monitoring) capability to ensure the cloud system maintains and acceptable risk posture.

(4) Implement an ongoing A&A and Authorization plan to cover security and privacy incident response and mitigation capabilities. After operation commences on a CSP system, follow the FedRAMP ongoing A&A processes.

(5) The FedRAMP requirements provide the necessary elements to ensure that VA and the CSP have a fully implemented ongoing A&A capability in accordance with all DHS guidance.

(6) If the cloud service maintains a provisional ATO with the FedRAMP JAB, the FedRAMP PMO will assign an ISO who will coordinate continuous monitoring between the service provider and VA. These artifacts will be available to all organizations that leverage the service. If the cloud service maintains only an Agency ATO from VA, VA is responsible for ensuring the proper continuous monitoring artifacts are submitted to VA and reviewed.

(7) The CSP, FedRAMP, and VA share the responsibility for continuous monitoring of the cloud based information system.

(8) The processes and tasks that will be performed in this step are:

(a) Maintain Operational Visibility:

1. Establish data feeds from CSP systems to VA monitoring systems;

2. Conducting Annual Self-Attestation;

3. Ensuring the CSP Risk Posture meets VA's ATO requirements;

4. Perform Contract Management by monitoring service agreement, and monitoring service levels; and

5. Perform annual security assessment to determine new risks to the system.

(b) Perform Change Control:

1. Obtain Change Reports/POA&M Updates. Update of POA&M contains system owner “to do” list for mitigating security weaknesses;

2. Ensure POA&M/System Changes meet FedRAMP Provisional Authorization, and VA ATO requirements;

3. Update SSP to include changes in control implementations. The SSP should be reviewed at least annually;

4. Update IT Contingency Plan (ITCP) to reflect contingency plan changes;

5. Update Separation of Duties Matrix. User roles are reviewed to ensure separation of duties;

6. Update Configuration Management Plan to reflect changes in the Configuration Management process; and

7. Update CSP IT Security Policies.

(c) Perform Incident Response:

1. Automatically submit incident notifications;

2. Respond to incidents;

3. Coordinate with US-CERT in accordance with the timeframes in the Incident Response Plan;

4. Submit Incident Response Test Report resulting from annual test of Incident Response Plan; and

5. Submit Physical Access Review Report detailing physical access to CSP data centers.

(d) **Perform Vulnerability and Penetration Testing: -** Perform Vulnerability scans that test security controls for vulnerabilities;

6. RESPONSIBILITIES

The responsibilities listed below are specific responsibilities related to A&A of cloud computing services. For overall information security program responsibilities for these positions, see VA Directive and Handbook 6500.

a. **Secretary of Veterans Affairs** has designated the Chief Information Officer (CIO) as the senior Agency Official responsible for ensuring enforcement and compliance with the requirements imposed on VA under FISMA and FedRAMP.

b. **Assistant Secretary for Information and Technology**, as VA's CIO, is responsible for:

(1) Recommending VA information systems migrate to cloud technologies whenever possible and if cost effective in accordance with OMB Circular No. A-94, Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs;

(2) Assuming the responsibility, as the Authorizing Official (AO), to ensure information systems operate at an acceptable level of risk;

(3) Assessing, authorizing, and continuously monitoring the overall program for security controls, including FedRAMP security controls, within VA's area of responsibility;

(4) Establishing policies and procedures that promote effective and secure cloud computing services to support the Federal CIO's mission for secure, cost-saving technological innovations to support VA's infrastructure, information systems, and data repositories;

(5) Delegating daily operations and maintenance responsibilities to OI&T officials so they may obtain internal A&A for private cloud services as well as leverage and approve other agency and provisional A&A from the Joint Authorization Board (JAB) for Public Cloud, Community Cloud, or Hybrid Cloud deployment models;

(6) Requiring that CSPs route their traffic such that the service meets the requirements of the TIC program in accordance with DHS guidance and VA Directive 6513, Secure External Connections;

(7) Ensuring that acquisition requirements address maintaining FedRAMP security authorization requirements and that relevant contract provisions related to contractor reviews and inspections are included for CSPs;

(8) Evaluating and approving, approving with contingencies, or disapproving VA business use cases including reviewing the business use cases for cost effectiveness and feasibility;

(9) Obtaining advice from FedRAMP for Public Cloud, Community Cloud, or Hybrid Cloud deployment models, as needed, for best practice implementation of selected business use cases prior to submission for A&A;

(10) Providing an annual report to the Federal CIO on cloud services that have been implemented and include the rationale for exclusion of systems that cannot meet FedRAMP requirements;

(11) Establishing and implementing an incident response and mitigation capability for security and privacy incidents for cloud services in accordance with DHS guidance and VA Handbook 6500; and

(12) Using the FedRAMP Program Management Office (PMO) process and the JAB-approved FedRAMP security authorization requirements as a baseline when initiating, reviewing, granting and revoking security authorizations for cloud services.

c. **Deputy Assistant Secretary (DAS) for Information Security**, as the VA Chief ISO is responsible for:

(1) Ensuring VA information security policies and procedures are consistent with Federal laws and guidance, VA regulations and policies, and FedRAMP requirements;

(2) Developing VA information security policies and procedures consistent with Federal laws and guidance, and VA regulations and policies to support the Cloud First initiative and ensure compliance with the FedRAMP A&A process;

(3) Ensuring compliance with integrating the low and moderate baseline security controls in cloud systems as required by FedRAMP;

(4) Applying guidance, templates, and other artifacts when necessary to protect VA assets, and adding any additional security controls for agency-specific needs;

(5) Approving the preliminary cost benefit justification for the business use case from DAS;

(6) Accept or reject CSP's FedRAMP Provisional ATO;

(7) Accept or reject CSP's A-ATO from other federal agencies; and

(8) Approving the preliminary risk assessment of the business use case.

d. **Deputy Chief Information Officer for Architecture, Strategy, and Design (ASD)** is responsible for:

(1) Ensuring, when input is requested, that approved cloud computing initiatives align with the VA Enterprise Technical Architecture, including Enterprise Design Patterns, Technical Reference Model (TRM), and the Enterprise Technology Strategic Plan (ETSP);

(2) Providing service intermediation among the lines of business using an enterprise wide cloud broker capability;

(3) Establishing Standardized Service Creation and Infrastructure Contracting with Technical Assistance Center. Develop Standard Contract language that incorporates the enterprise standard cloud solutions as Government Furnished Equipment (GFE) in conjunction with Technical Assistance Center;

(4) Supporting the development of Standard Contract language for cloud service integration, brokerage, and monitoring;

(5) Assisting Technical Assistance Center and others to establish consumption based contracting and service delivery models;

(6) Creating enforceable Enterprise Design Patterns that provide architectural principles and constraints for deriving CSP integration architectures in accordance with VA security and privacy policies;

(7) Defining portability standards for migrating activities to and from a CSP;

(8) Establishing the framework needed to broker services to satisfy business needs that enable application sustainment and portability

(9) Evaluating business requirements against Enterprise Shared Services (ESS) in accordance with Enterprise Design Pattern

(10) Ensuring the One-VA Technical Reference Model (TRM) includes a catalog of approved standards and technologies to support integration with cloud services;

(11) Defining and evolving pertinent IT vision attributes for cloud computing and infrastructure in the Enterprise Technology Strategy Plan (ETSP) managed by ASD Technology Strategies;

(12) Utilizing an enterprise-level cost modeling approach for strategic and tactical product planning that incorporates CSPs in accordance with the ProPath Business Needs Intake and Analysis (BNIA) process;

(13) Maintaining a service catalog of all current and planned CSPs for use in both short-term and log-term planning and utilization;

(14) Facilitating development of implementation guidelines for short-term, mid-term, and long-term cloud computing objectives;

(15) Supporting development of an acquisition plan for cloud migration in conjunction with ASD, EPMO, and contracting (Technical Assistance Center);

(16) Updating IT governance charters (Enterprise Architecture Council) Architecture and Engineering Review Board (AERB) and Enterprise Technical Architecture Work Group)) as needed to account for inclusion of CSPs in the VA ETA (AERB) and Enterprise Technical Architecture Work Group (ETAWG)) and operating guides;

(17) Developing and reviewing an enterprise risk management framework in support of cloud migration;

(18) Identify changes needed to Project Management Account System and ProPath to support cloud migration;

(19) Representing a person or organization that maintains a business relationship with, and uses the service from a cloud provider;

(20) Browsing the service catalog from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service;

(21) The cloud consumer may be billed for the service provisioned, and needs to arrange payments accordingly;

(22) Reviewing the preliminary risk assessment of the business use case; and

(23) Submitting the preliminary risk assessment to the DAS for Information Security to review and approve.

e. **Deputy Assistant Secretary, Enterprise Program Management Office (EPMO)** is the chief advisor to AS/IT for all enterprise application development activities. Development consists of planning, developing (or acquiring), and testing applications that meet business requirements. As the central cloud consumer for VA, EPMO's responsibilities include:

(1) Support Technical Working Groups to standardize Cloud Service Deployment across the OI&T Pillars in coordination with the technical cloud broker;

(2) Support the development and implementation of standardized Service Creation and Infrastructure Contracting with Technical Assistance Center;

(3) Develop and track application Performance criteria;

(4) Develop Standard Contract language for cloud computing performance and that requires contractors to follow ASD design patterns and portability standards in coordination with Technical Assistance Center;

(5) Support development of an acquisition plan for cloud migration in conjunction with ASD, SDE and the Technical Assistance Center;

(6) Support Office of Information Security (OIS), to ensure application level ATO process standards and POA&M requirements are met;

(7) Developing and maintain a Catalogue of Enterprise Cloud Services;

(8) Leading Technical Working Groups to standardize Service Deployment across the OI&T Pillars in coordination with the technical cloud broker; and

(9) With OIS, ensuring ATO process standards and POA&M requirements are met.

f. **Chief Financial Officer (CFO) for Information Technology Resource Management (ITRM)** is responsible for:

(1) Evaluating resource requirements in support of cloud services including assessing the cost estimates, cost-benefit analysis, cost effectiveness, and resources required for supporting a cloud service; and

(2) Submitting the preliminary risk assessment for approval from DAS for Information Security.

g. **Deputy Assistant Secretary for Service Delivery and Engineering (SDE)** is responsible for developing, procuring, integrating, modifying, maintaining, and implementation of security over VA information and information systems, and as the VA Technical Cloud Broker, manages the use, performance, and delivery of cloud services, and negotiates relationships Responsibilities include:

(1) Implementing the procedures in this handbook and any subsequent guidance document that may be required, including ensuring VA Information System Owners are provided the resources and tools for oversight of security practices regarding cloud services;

(2) Assisting and coordinating with the VA information system owners in managing cloud computing services for VA information systems;

(3) 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);

(4) Providing services intermediation at the technical level;

(5) Providing service aggregation at the technical level in close coordination with EPMO;

(6) Providing service arbitrage at the technical level in close coordination with EPMO;

(7) Serving as Contracting Officer's Representative (COR) for Cloud Infrastructures, applications and platforms;

(8) Leading Technical Working Groups to standardize Cloud Service Deployment across the OI&T pillars;

(9) Supporting the development and implementation of standardized Service creation and Infrastructure contracting with the Technical Assistance Center;

(10) Developing standard SLAs for cloud services consistent with design patterns, portability standards and application performance requirements;

(11) Supporting development and enforce enterprise design patterns and portability standards for cloud services;

(12) Developing and maintain a Technical Catalogue of Enterprise Cloud Services;

(13) Overseeing development of an acquisition plan for cloud migration in conjunction with SDE, EPMO and contracting (Technical Assistance Center);

(14) Supporting OIS, to ensure infrastructure level ATO process standards and Plan of Action and Milestones (POA&M) requirements are met;

(15) Providing Centralized Capacity Management for Internal and External Capacity;

(16) Reviewing and evaluating business use cases from DAS for Information Security after approval of preliminary risk assessment and cost benefit justification prior to submission to VA CIO for risk acceptance and cost benefit approval;

(17) Ensuring the completion of needs assessment, feasibility evaluations, alternative solution analysis, cost-benefit analysis estimates and business use case reviews for cloud services;

(18) Reviewing and evaluating cloud deployment models for selected baseline security controls according to VA Handbook 6500;

(19) Ensuring internal cloud implementations and contract requests for a cloud service include the security categorization of the systems as defined in FIPS 199, procedures for change management requirements, configuration management compatibility, release management for the cloud service, and the inclusion of incident management, and continuous monitoring;

(20) Serving as an approval authority for the business use case following VA CISO's review; and

(21) Facilitating and coordinating divisional support and approval of technical requirements in cooperation with OI&T.

h. **Executive Director, Enterprise Operations** will report directly to the Assistant Secretary for Information and Technology and is responsible for:

(1) Managing all voice, data, video systems, and network transport throughout the enterprise including facilities; and

(2) Managing the budget, performing capacity planning for cloud services, and evaluating design of all communication systems; including the architectural infrastructure throughout the enterprise as a shared responsibility with Enterprise Systems Engineering.

i. **Enterprise Systems Engineering** is responsible for:

(1) Performing capacity planning for cloud services, and evaluating design of all communication systems; including the architectural infrastructure throughout the enterprise as a shared responsibility with the Office of Enterprise Operations.

j. The **Technology Acquisition Center in** the Office of Acquisitions Operations under the Deputy Secretary for Acquisitions and Logistics is part of the contracting, acquisition and procurement staff for VA. The Technology Acquisition Center is responsible for:

(1) Advising and providing guidance to senior leaders regarding acquisition strategy and issues and provides acquisition, contracting and procurement support to Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), National Cemetery Administration (NCA), OI&T, and Veterans Affairs Central Office (VACO) staff;

(2) Providing dedicated acquisition and program management expertise and support for life cycle management of enterprise wide solutions in information and technology, primarily for the OI&T;

(3) Working closely with the business and technical cloud broker and the central cloud consumer;

(4) Supporting the development and implementation of standardized Service Creation and Infrastructure Contracting;

(5) Developing Standard Contract language for cloud computing performance that requires contractors to follow ASD design patterns and portability;

(6) Supporting development of an acquisition plan for cloud migration in conjunction with ASD, SDE and EPMO;

(7) Assisting the development and implementation of consumption based contracting and service delivery models;

(8) Establishing Standardized Service Creation and Infrastructure Contracting. Develop Standard Contract language that incorporates the Enterprise standard cloud solutions as GFE;

(9) Supporting the development of Standard Contract language for cloud computing by technical broker, central Cloud consumer and contracting;

(10) Supporting SDE as COR for Cloud Infrastructures, applications and platforms;

(11) Supporting the development and implementation of standardized Service creation and Infrastructure contracting with the Technology Acquisition Center; and

(12) Developing standard SLAs for cloud services consistent with design patterns, portability standards and application performance requirements.

k. **Information/Business Owners (e.g., VHA, VBA, and NCA)** are responsible for:

(1) Providing business mission requirements and needs for possible cloud services within their Administration;

(2) Assisting in evaluating and determining the security controls necessary to include in cloud computing initiatives that involve Protected Health Information (PHI) or other VA sensitive information; and

(3) Preparing and submitting a cost effective business use case for review by the VA CIO for consideration of cloud technology for a business/mission request.

l. **VA-Network Security Operations Center (NSOC)** is responsible for:

(1) Ensuring all connections to the cloud are compliant using current VA-NSOC approved processes;

(2) Evaluating and testing the performance of cloud services based on VA-NSOC's operating requirements;

(3) Working with system owners and local system/network administrators;

(4) Coordinating all efforts related to TIC and CSP interconnection;

(5) Ensuring operations, engineering, and maintenance of the four VA trusted Internet connection gateways. All cloud connections must connect to at least one VA trusted Internet connection gateway via a business partner extranet connection; and

(6) Performing vulnerability and penetration testing as part of the continuous monitoring of VA's private cloud services.

m. **Information System Owners** are responsible for:

(1) Reporting, documenting, and ensuring all cloud services are secured within the Information System Owner's area of responsibility;

(2) Identifying the security categorization of the systems as defined in FIPS 199, procedures for change management requirements, configuration management compatibility, release management for the cloud service, and the inclusion of incident management, and continuous monitoring;

(3) Creating, maintaining and submitting cloud service change requests for continuous monitoring, implementation, or maintenance for approval to the ESCCB;

(4) Completing cloud system questionnaires in RiskVision;

(5) Uploading CSAR assessment of CSP accreditation package into RiskVision;

(6) Ensuring CSP's system has developed a secure baseline of security controls by scoping, tailoring, compensating, and supplementing the controls as outlines in VA Handbook 6500;

(7) Obtaining Memorandum of Understanding/Interconnection Security Agreements (MOU/ISA) when needed from the FedRAMP PMO for adaptation to systems for outsourced cloud services that have obtained provisional A&A;

(8) Ensuring all required security controls for which VA is fully or partially responsible are documented in the appropriate internal VA system security documentation. This includes generation of an internal VA System Security Plan (SSP) that details the control implementation of VA responsibilities; and

(9) Using FedRAMP when conducting risk assessments, security authorizations, and granting ATOs for all Executive department or agency use of cloud services.

n. **Local CIOs/System Administrators/Network Administrators** are responsible for:

(1) Assisting and coordinating with VA Information System Owners in establishing and submitting cloud service requirements for VA information systems;

(2) Assisting and coordinating with VA Information System Owners in creating, maintaining and submitting cloud service change requests for continuous monitoring, implementation, or maintenance for approval to the ESCCB;

(3) Assisting and coordinating with VA Information System Owners in the maintenance of all cloud services and assessing the security control implications for VA information systems;

(4) Assisting and coordinating with VA Information System Owners in managing cloud services; and

(5) Creating change requests that describe how controls must be adjusted in order to maintain security and functionality of cloud services and submitting the change requests to the ESCCB to evaluate and test periodically.

o. **Information Security Officers (ISO)** are responsible for:

(1) Managing the security program under their area of responsibility including assessment of risk according to security categorization;

(2) Ensuring security baseline compliance for all cloud systems;

(3) Complete cloud system questionnaires in RiskVision;

(4) Review CSP accreditation package for approval; and

(5) Coordinating system security plan requirements with Information System Owners.

p. **Certification Program Office (CPO)** is responsible for:

(1) Determine if FedRAMP Provisional ATO addresses and complies with VA, DHS TIC requirements; and

(2) Review CSP accreditation package for completeness;

q. **Contracting Officer (CO)** are responsible for:

(1) Ensuring that security requirements and security specifications are explicitly included in VA contracts, as per requiring or program direction;

(2) Coordinating contract documentation with the ISO and PO to ensure that contracts contain the required security language necessary for compliance with FISMA, and 38 U.S.C. §§ 5721-5728, and to provide adequate security for information and information systems used by the contractor, including the requirement to take VA's annual information security training on at least an annual basis and sign a VA Contractor ROB on an annual basis, whenever a contractor will be using VA information or information systems;

(3) (c) Monitoring COR surveillance to ensure contract requirements for contractors meet the appropriate background investigation requirements in accordance with VA Directive and Handbook 0710;

(4) Monitoring COR surveillance to ensure contractors complete VA's security and privacy awareness training and additional role-based training, as outlined in the contract;

(5) Monitoring COR surveillance of the contract to ensure security requirements are being met, consulting the ISO and/or PO as necessary; and

(6) Assisting other VA officials with significant information security responsibilities in remediating the weaknesses or deficiencies identified in the POA&M; updating the POA&M, conducting periodic compliance validation reviews, and completing the FISMA annual assessment to reduce or eliminate system vulnerabilities.

r. **Contracting Officer's Representative (COR)** are responsible for:

(1) Working with the ISO and PO to ensure contracts contain the required security language necessary for compliance with FISMA and 38 U.S.C. §§ 5721-5728 and to provide adequate security for information and information systems used by the contractor, including the requirement for signing VA Contractor ROB, when applicable;

(2) Ensuring contract requirements for contractors meet the appropriate background investigation requirements in accordance with VA Directive and Handbook 0710;

(3) Ensuring contractors complete VA's security and privacy awareness training and any additional role-based training, as outlined in the contract; and SOP; and

(4) Monitoring of the contract to ensure that security requirements are being met, consulting the ISO and/or PO as necessary.

This page is intentionally blank for the purpose of printing front and back copies.

APPENDIX A. TERMS AND DEFINITIONS

1. **Assessment and Authorization (A&A):** The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to VA operations (including mission, functions, image, or reputation) and assets, or individuals, based on the implementation of an agreed-upon set of security controls. SOURCE: SP 800-37

2. **Authorization to Operate (ATO):** The official management decision given by a senior organizational official, after completing a security assessment, to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. SOURCE: SP 800-37

3. **Authorizing Official (AO):** Senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. In VA, this is the VA CIO. SOURCE: SP-800-53; SP 800-53A; SP 800-37

4. **Community Cloud:** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. SOURCE: SP 800-145

5. **Concept of Operations:** A security-focused description of an information system, its operational policies, classes of users, interactions between the system and its users, and the system's contribution to the operational mission. SOURCE: CNSSI 4009

6. **Control Implementation Summary:** A document that summarizes security control ownership and indicates which controls are owned and managed by the CSP and which controls are owned and managed by the leveraging agency. SOURCE: FedRAMP Concept of Operations v. 1.0

7. **Control Tailoring Workbook (CTW):** A document used by the CSP to document their security control implementation and define their implementation settings for FedRAMP defined parameters and any compensating controls. SOURCE: FedRAMP Concept of Operations v. 1.0

8. **Cloud Computing:** A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. SOURCE: SP 800-145

9. **Cloud Consumer:** A government agency requiring or using cloud computing services.

10. **Cloud Service Provider (CSP):** a commercial or government agency providing cloud computing services.

11. **Continuous Monitoring:** Maintaining ongoing awareness to support organizational risk management decisions. Monitoring includes, but is not limited to, assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated agency officials on an ongoing basis. See Information Security Continuous Monitoring. SOURCE: OMB Cir. A-130, SP 800-137

12. **External Entities:** Organizations that are outside of VA such as other government agencies, private industry organizations, and the general public. Internal VA administrations (Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA)) are not considered external entities.

13. **FedRAMP:** A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP uses a "do once, use many times" framework that will save cost, time, and staff required to conduct redundant agency security assessments. SOURCE: FedRAMP Concept of Operations v. 1.0

14. **Hybrid Cloud:** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (Private Cloud, Community Cloud, or Public Cloud) that remain unique identities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). SOURCE: SP 800-145

15. **Infrastructure as a Service (IaaS):** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). SOURCE: SP 800-145

16. **Information Owner:** Agency official with statutory or operational authority for specified information and responsibility for establishing the criteria for its creation, collection, processing, dissemination, or disposal, which responsibilities may extend to interconnected systems or groups of interconnected systems. SOURCE: 38 U.S.C § 5727(9)

17. **Information System:** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual. SOURCE: 38 U.S.C. § 5727.

18. **Information Resources:** Information in any medium or form and its related resources, such as personnel, equipment, funds, and IT. SOURCE: 38 U.S.C § 5727

19. **Information Security Officer (ISO):** Individual working with the senior agency ISO, AO, or Information System Owner to help ensure the appropriate operational security posture is maintained for an information system or program. SOURCE: CNSSI 4009 [VA Adapted]

20. **Information System Owner:** Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. SOURCE: FIPS 200

21. **Information Technology (IT):** Any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. SOURCE: SP 800-53; SP 800-53A

22. **Interconnection Security Agreement (ISA):** An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) between the organizations. SOURCE: NIST SP 800-47

23. **Joint Authorization Board (JAB):** Primary governance and decision-making body for the FedRAMP program. Reviews and provides joint provisional security authorizations of cloud solutions using a standardized baseline approach. SOURCE: GSA.gov

24. **Managed Services:** An external information system service that is implemented outside of the authorization boundary of a VA information system that includes services are used by, but not part of, VA information systems. SOURCE: VA Handbook 6500

25. **Memorandum of Understanding (MOU):** A document established between two or more parties to define their respective responsibilities in establishing, operating, and securing a system interconnection. SOURCE: NIST SP 800-47

26. **OI&T Pillar:** Office of Information and Technology Organizational Element.

27. **Platform as a Service (PaaS):** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. SOURCE: SP 800-145

28. **Private Cloud:** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. SOURCE: SP 800-145

29. **Provisional Authorization to Operate:** A provisional authorization is an initial statement of risk and approval of an authorization package by the JAB pending the issuance of an agency ATO by the Executive department or agency acquiring the cloud service. SOURCE: FedRAMP JAB Charter

30. **Public Cloud:** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. SOURCE: SP 800-145

31. **Risk:** The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. SOURCE: SP 800-60

32. **Risk Assessment:** Process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other operations, and the Nation, arising through the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. SOURCE: SP 800-53; SP 800-53A; SP 800-37

33. **Risk Management:** The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system; and (iv) documenting the overall risk management program. SOURCE: SP 800-53; SP 800-53A; SP 800-37

34. **Security Assessment Plan (SAP):** A plan that provides the objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment. SOURCE: NIST SP 800-37

35. **Security Controls:** The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. SOURCE: SP 800-53; SP 800-37; SP 800-53A; SP 800-60; FIPS 200; FIPS 199

36. **Software as a Service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser

(e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. SOURCE: SP 800-145

37. **System Security Plan (SSP)**: A plan that defines the security controls that are either planned or implemented for networks, facilities, systems, or groups of systems, as appropriate, within a specific accreditation boundary. SOURCE: 38 U.S.C. § 5727

38. **System Development Life Cycle (SDLC):** The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal. SOURCE: CNSSI 4009

39. **Third Party Assessment Organizations (3PAO):** Independently performs security assessments of CSP systems and creates security assessment package artifacts in accordance with FedRAMP requirements.

40. **Trusted Internet Connection (TIC):** A secure connection between and agency system and an external system routed through an approved TIC gateway.

This page is intentionally blank for the purpose of printing front and back copies.

APPENDIX B. ACRONYMS AND ABBREVIATIONS

Acronym/ Abbreviation	Definition
3PAO	Third Party Assessment Organization
A&A	Assessment and Authorization
AERB	Architecture Engineer Review Board
AO	Authorizing Official
ASD	Architecture Strategy and Design
ATO	Authorization to Operate
BIA	Business Impact Analysis
BNIA	Business Needs Intake and Analysis
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIS	Control Implementation Summary
CNSSI	Committee on National Security Systems Instruction
CO	Contracting Officer
COR	Contracting Officer's Representative
CPO	Certification Program Office
CSP	Cloud Service Provider
CTW	Control Tailoring Workbook
DAS	Deputy Assistant Secretary
DHS	Department of Homeland Security
EPMO	Enterprise Program Management Office
ESCCB	Enterprise Security Change Control Board
ETAWG	Enterprise Technical Architecture Working Group
ESS	Enterprise Shared Services
ETSP	Enterprise Technology Strategic Plan
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
GFE	Government Furnished Equipment
GSA	General Services Administration
IaaS	Infrastructure as a Service
ISO	Information Security Officer

Acronym/ Abbreviation	Definition
IT	Information Technology
JAB	Joint Authorization Board
ITRM	Information Technology Resource Management
MOU/ISA	Memorandum of Understanding/Interconnection Security Agreement
NCA	National Cemetery Administration
NIST	National Institute of Standards and Technology
NSOC	Network and Security Operations Center
OIS	Office of Information Security
OI&T	Office of Information and Technology
OMB	Office of Management and Budget
PaaS	Platform as a Service
PHI	Protected Health Information
PMO	Program Management Office
POA&M	Plan of Action and Milestones
PTA	Privacy Threshold Analysis
SaaS	Software as a Service
SAP	Security Assessment Plan
SAR	Security Assessment Report
SDOC	Supplier’s Declaration of Conformity
SDE	Service Delivery and Engineering
SDLC	System Development Life Cycle
SP	Special Publications
SSP	System Security Plan
TIC	Trusted Internet Connection
VA	Department of Veterans Affairs
VACO	Veterans Affairs Central Office
VBA	Veterans Benefits Administration
VHA	Veterans Health Administration

APPENDIX C. REFERENCES

1. Federal Information Processing Standards (FIPS) Publications

a. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems, February 2004*

b. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006

2. National Institute of Standards and Technology (NIST) Special Publications (SP)

a. NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

b. NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*

c. NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*

d. NIST SP 800-145, *The NIST Definition of Cloud Computing*

3. Office of Management and Budget (OMB) Publications

a. OMB Circular No. A-94*, Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs*

b. OMB Circular No. A-130, *Managing Information as a Strategic Resource*

4. Department of Homeland Security (DHS) Publications

a. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2

5. VA Directives and Handbooks

a. VA Directive 6517, *Cloud Computing Services*

b. VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*

c. VA Handbook 6500.3, *Assessment, Authorization, and Continuous Monitoring of VA Information Systems*

d. VA Handbook 6500.5, *Incorporating Security and Privacy into the System Development Life Cycle*

e. VA Handbook 6500.6, *Contract Security*

f. VA Directive 6513, *Secure External Connections*

6. Other References

a. U.S. Chief Information Officer, *Federal Cloud Computing Strategy*, dated February 8, 2011

b. FedRAMP Concept of Operations