**VISTA Adaptive Maintenance:**

**System Boundaries and Data Flows**

March 5, 2018

**Introduction**

The VISTA Adaptive Maintenance (VAM) project provides a cloud-based roadmap and software for maintaining VISTA and the VA workflows it supports in an efficient, cost-effective manner during the multi-year transition to VA’s new commercial EHR. VAM enables VA to move from 130 separate, complex, unmaintainable VISTA systems to a single, secure, commercially-managed set of centralized cloud-based services - Veteran Integrated Care Services (VICS) - while maintaining the full continuity of care and workflows of the current clinical client, CPRS. VAM will be hosted in production within the VA’s Enterprise Cloud (VAEC) using Amazon Web Services (AWS).

**Security Boundaries**

***There are three security boundaries:***

1. **VAM Boundary:** VAM and its associated components (VICS Server and Datastore, RPC Router, Router Manager) are all contained within a single security boundary (“black box”) within the VAEC using the AWS VA General Support System (GSS) controls that are already documented within Risk Vision. All Security controls that are already documented in Risk Vision for AWS GSS cloud will be inherited within our System Security Plan (SSP). VAM will connect directly to the Client Boundary and the VISTA Boundary through the VA Business Partner Extranet (BPE).

2. **Client Boundary:** The clinical client (CPRS for the IOC) will be run on a machine within the end-user’s segment of the VA network (at the IOC Site). It will directly connect to the VAM Boundary through the VAECs Business Partner Extranet (BPE) ExpressRoute connection.

3. **VISTA Boundary**: The VISTA instance is an OIT-endorsed and secured Test VISTA deployed within VA’s network. The Router is configured to talk to this VISTA within the VAM Boundary through the VA Business Partner Extranet (BPE).

***The VAM Boundary contains three components:***

1. **Veteran Integrated Care Services (VICS) Server:** This provides the centralized datastore and business logic for all services.
2. **RPC Router (“Router”)**: The Router receives RPC requests from clients (e.g. CPRS) and routes the RPC call to either the VISTA Server (RPC pass-through) or to the cloud-based VICS Server (RPC emulated).
3. **RPC Router Manager (“Router Manager”):** Manages configuration and auditing of the RPC Router. The RPC Router Manager can be accessed securely via encrypted web browser client.

All components within the VAM Boundary will be managed within a single security boundary within VAEC.

**Data Flows**

***VAM is a ‘black box’ with four external data flows (interfaces) as follows:***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Data Flow** | **Type** | **Connection** | **VAM Boundary** | **Security Controls** |
| 1 | Router - CPRS  (Clinical client) | Read-write RPCs | ***Encrypted*** | BPE Express Route | AWS GSS cloud |
| 2 | Router - Router Manager  (Management client) | Read-write REST | ***Encrypted*** | BPE Express Route | AWS GSS cloud |
| 3 | Router - VISTA  (Clinical server) | Read-write RPCs |  | BPE Express Route | AWS GSS cloud |
| 4 | VICS Server - VISTA Server  (Metadata sync) | Read-only RPC  (One-off Batch job) |  | BPE Express Route | AWS GSS cloud |



**Figure 1. VISTA Adaptive Maintenance (VAM)**

**Security Boundaries and Data Flows**