**VISTA Adaptive Maintenance:**

**System Boundaries and Data Flows**

**OIT RiskVision Review**

March 6, 2018

**Introduction**

The VA *VISTA* Adaptive Maintenance (VAM) is a Veteran-focused Integration Program (VIP) that 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 transition from 130 separate, complex VISTA systems to a single, secure, commercially-managed set of centralized cloud-based services - Veteran Integrated Care Services (VICS) - while maintaining full backwards-compatibility and continuity of care and workflows of the Computerized Patient Record System (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, Router, Router Manager) are all contained within a single security boundary 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 via the VA Business Partner Extranet (BPE).

2. **Client Boundary:** The client (CPRS) will be run on a machine within the end-user’s segment of the VA network (at the IOC Site). The client will connect across the VAM Boundary using 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 across the VAM Boundary through the VA Business Partner Extranet (BPE).

***The VAM Architecture contains three components:***

1. **Veteran Integrated Care Services (VICS) Server:** This server provides the centralized data store 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 passes through) or to the cloud-based VICS Server (RPC is emulated) or both (write RPCs go to both targets).
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 has four data flows as follows:***

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



Figure 1. VISTA Adaptive Maintenance (VAM)

Security Boundaries and Data Flows

**Abbreviations**

|  |  |  |
| --- | --- | --- |
| **Abbreviation** | **Definition** | **Link** |
| VISTA | Veteran Information System Technology Architecture | https://en.wikipedia.org/wiki/VistA |
| CPRS | Computerized Patient Care System | https://www.va.gov/vdl/application.asp?appid=61 |
| VAM | VISTA Adaptive Maintenance | http://vistaadaptivemaintenance.info |
| RPC | Remote Procedure Call | https://en.wikipedia.org/wiki/Remote\_procedure\_call |
| VICS | Veteran Integrated Care Services | http://vistaadaptivemaintenance.info |
| AWS | Amazon Web Services | https://en.wikipedia.org/wiki/Amazon\_Web\_Services |
| RiskVision | Tool for security risk assessment; acquired by Resolver. | https://www.resolver.com/risk-vision-information-security-software |
| GRC | Governance Risk and Compliance | https://en.wikipedia.org/wiki/Governance,\_risk\_management,\_and\_compliance |
| FIPS | Federal Information Processing Standards | https://en.wikipedia.org/wiki/Federal\_Information\_Processing\_Standards |
| FISMA | Federal Information Security Management Act | https://en.wikipedia.org/wiki/Federal\_Information\_Security\_Management\_Act\_of\_2002 |
| VAEC | VA Enterprise Cloud | See: AWS |
| VIP | Veteran-focused Integration Program | https://www.osehra.org/sites/default/files/VIP\_Guide\_1\_0\_v14.pdf |
| IOC | Initial Operating Capability |  |
| SSP | System Security Plan |  |
| ATO | Authority to Operate |  |