|  |  |  |  |
| --- | --- | --- | --- |
| Department of Veterans Affairs | | | Memorandum |
| Date: | January 28, 2019 |  | |
| From: | John P. Elliott—V2EC System Owner | | |
| Subj: | Request for Approval: V2EC Data Transfer to VA Enterprise Cloud S3 | | |
| To: | Deputy Assistant Secretary Bill James | | |

1. **Purpose Statement:**  In anticipation St Louis, Missouri (SMO) Defense Enterprise Computing Center (DECC) closure in early 2020, which currently hosts seventy Veteran Information System Technology Architecture (VistA) systems, the VA Office of Information and Technology (OI&T) Enterprise Cloud Solutions Office (ECSO), as the technology agent for the Veterans Health Administration (VHA), is providing migration and continuity of services for these VistA systems within the VA Enterprise Cloud (VAEC) under the VistA to Enterprise Cloud (V2EC) migration project.

The initial and most critical step of the VistA to Enterprise Cloud migration is the secure and efficient transfer of a VistA Test System (with its associated Veteran data) from the SMO DECC to a secured environment within the VAEC-managed AWS GovCloud. The VAEC AWS GovCloud provides a Server Migration Service (SMS) and Simple Storage Service (S3) for the efficient, automated secure transfer, storage, and migration of a server to AWS GovCloud. The transfer of the VistA server from SMO DECC to the VAEC will leverage these mechanisms, however will also include a Trusted Internet Connection (TIC) for the direct connection to SMO DECC, and will transfer the VistA image from S3 storage to the Virtual Private Cloud (VPC) immediately after the image is received in S3. The use of the S3 storage, however, requires executive approval. This memorandum requests the formal approval for the use of the VAEC-managed AWS GovCloud S3 storage as an approved method to receive the required VistA systems and data directly (via the TIC) from the SMO DECC.

2. **Recommendation:** The V2EC Program Office has assessed the options available to complete this data transfer and recommends the use of the S3 bucket to ensure secure, timely delivery of Veteran data while saving VA time and personnel resources. The use of the S3 bucket will be restricted to 1-day windows and used to migrate site data that are too large to migrate using Secure File Transfer Protocol (SFTP). The S3 bucket will be used as an option to migrate hospital and clinic site data when migration file sizes exceed ~1 TB.

3. **Current options approved by the VA:** The following VA Policies and Memos: Memo Subject External Connections through TIC (VAIQ# 7615078) dated July 10, 2015, VA Handbook 6500, and VA Handbook 6513, require that V2EC utilize established secure paths of data movement through the TIC Gateway between the VA and the Internet. The two paths currently available through the TIC are the delivery of a hard disk drive (HDD) to the Austin Information Technology Center (AITC) to load to the AWS GovCloud S3 Bucket or to transfer through a SFTP into the VA network.

4. **Why HDD delivery is not an option:** HDD delivery to AITC will not be able to support the strict timelines during the transition periods. The time required to create the drives, ship, and download the data will require 7 to 14 days. In addition, HDD delivery will require the movement of the drives through courier services resulting in the additional cost of having the data loaded to the same S3 bucket in the AWS GovCloud by AITC staff.

5. **Why SFTP is not an option:** SFTP transfer of the data will not be able to support the volume of data being transferred for larger sites or multi-site hosts such as Omaha. SFTP is generally configured to limit the size of files being moved due to the network constraints of the connection and would require establishing a permanent connection to move large data from larger facilities. At this time, V2EC does not have a Memorandum of Understanding-Interconnection Security Agreement (MOU/ISA) in place to allow such a permanent connection.

6. **How the S3 Bucket resolves the problems with HDD and SFTP and meets program objectives:** The FedRAMP High GovCloud S3 bucket provides for the timely, secure delivery of the necessary data load by removing many of the steps involved in HDD delivery. The GovCloud S3 bucket provides a faster load than SFTP, requiring less than one day to load ~1 TB of data. It accepts files up to 5 TB in size, optimizes file transfer by using multipart simultaneous uploads, and includes a file transfer manager that will prevent the corruption of files in the event that connection is lost during the transfer. The S3 bucket will only be available for use during a 24-hour window for each transfer period, after which all vendor accounts will be disabled and the S3 bucket will be inactivated if the transfer/data drop is successful. Considering the limited timeframe and temporary nature of the S3 bucket, the Enterprise Security External Change Council has determined that a Plan of Action and Milestones, approved by the V2EC Information System Security Officer, may be utilized if a timely MOU/ISA is not possible with V2EC.

7. **Identified risks with using the AWS GovCloud S3 bucket:**

Logical access: Connections to the AWS GovCloud S3 bucket will be via the public Internet to a .com top-level domain instead of .gov.

Network security: Connections to the S3 bucket will not be routed through a VA-managed access point (TIC) for monitoring.

Security misconfiguration: An accidental or deliberate change by an administrator could change the access restrictions to the S3 bucket from private access to public access.

8. **Compensating security controls to ensure protection of Veteran data:**

AC-2: Account Management:

• Access control mechanisms for S3 will be in place for both external user accounts (restricted to specific individuals at V2EC) and internal users (V2EC system administrators), activated only when necessary and deactivated when no longer required.

AC-3: Access Enforcement:

• An access control list configured in the S3 bucket will enforce access for V2EC users, which will limit their capabilities strictly to uploading data.

AC-4: Information Flow Enforcement:

• An ACL will restrict external access to the S3 bucket to allow only network traffic originating from V2EC source Internet Protocols.

AC-6: Least Privilege:

• V2EC system administrators must explicitly grant access to S3. Once they have assigned access via a policy attached to the V2EC users accounts, a separate policy will be attached to permit only V2EC users to upload data to the V2EC S3 bucket.

AC-17: Remote Access:

• Access to the S3 bucket will be via a Hypertext Transfer Protocol Secure (HTTPS) AWS GovCloud endpoint that uses Federal Information Processing Standards (FIPS) 140-2 validated cryptographic modules.

AC-21: Information Sharing:

• VA and V2EC will have formal, signed agreements in place detailing the specifics of the data transfer via S3.

AU-2: Audit Events:

• S3 logs all access requests, including: bucket, bucket owner, time, remote IP, requester ID, request ID, operation, key, request uniform resource indicator, HTTP status, error codes, bytes sent, object size, total time, turn-around time, referred, user-agent, and version ID.

• S3 logs all actions on objects in the bucket, including: upload, delete, get, create, post, restore, put, and copy.

CA-3.E5: System Interconnections - Restrictions on External System Connections:

• V2EC system owners will restrict external connections to S3 using a whitelist to allow only V2EC source IPs.

CM-7: Least Functionality:

• V2EC system owners will configure the S3 bucket to provide only the essential capabilities required to provide V2EC with a secure location to upload files. Owners will encrypt objects as they are uploaded to the S3 bucket. By default, AWS S3 buckets are private with access restricted to the resource owner/root account (VAEC) and the AWS account that created the bucket (V2EC system administrators).

IA-2: Identification and Authentication:

• Access to all services in the VAEC AWS GovCloud, including S3, require the use of multi-factor authentication (MFA). V2EC system owners establish MFA during the account provisioning process requiring adding all users to the ‘force-MFA’ group per VAEC policy.

SC-8: Transmission Integrity:

• V2EC system administrators will encrypt all data in transit from V2EC to the S3 bucket using FIPS 140-2 compliant encryption. Accessing the S3 bucket will require V2EC to connect to a HTTPS AWS GovCloud endpoint, which uses FIPS 140-2 validated cryptographic modules for encryption.

SC-13: Cryptographic Protection:

• As the V2EC data transfer will consist of Veteran health data (Protected Health Information and Personal Identifiable Information), V2EC owners will configure the S3 bucket to meet cryptographic requirements for protecting privacy data in accordance with HIPAA, Federal and VA laws, directives, regulations, policies, and standards. V2EC system administrators will accomplish this by using FIPS 140-2 compliant encryption for data in transit and data at rest.

SC-28: Protection of Information at Rest:

• V2EC system owners will encrypt all at-rest data uploaded to S3 using Advanced Encryption Standard-256 encryption, which is enabled by default in S3.

9. **Summary:** The current approved options for transferring data to V2EC are insufficient for transferring the large volume of data needed to meet program requirements. The VAEC AWS GovCloud S3 bucket, and by extension the SMS, with managed compensating controls, is capable of providing the timely, secure transfer of data and server images to the V2EC VPC but requires executive approval for the first stage of the transfer from V2EC to AWS GovCloud since it does not traverse the TIC at this stage. Approval of this option will be limited to the scope of the V2EC project defined in Paragraph 2 above.

The point of contact for this memo is David Catanoso. He can be reached by phone, (732) 440-9583, or email Catanoso, David <David.Catanoso@va.gov>.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

John P. Elliott, V2EC System Owner

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Edgardo Rivera, Information System Security Officer

Approved: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Bill James, Deputy Assistant Secretary